BASES INTEGRADAS

Concurso de Méritos Nº 0004-2024-BN

SERVICIO DE IMPLEMENTACIÓN DE NUEVA PLATAFORMA BANCARIA PARA CANALES DIGITALES BANCA MÓVIL Y BANCA POR INTERNET DEL BANCO DE LA NACIÓN

2024

DEBER DE COLABORACIÓN

La Entidad y todo proveedor que se someta a las presentes Bases, sea como participante, postor y/o contratista, deben conducir su actuación conforme a los principios generales del derecho público que resulten aplicables al presente proceso de contratación.

En este contexto, se encuentran obligados a prestar su colaboración a la Secretaría Técnica de la Comisión de Defensa de la Libre Competencia del INDECOPI, en todo momento según corresponda a sus competencias, a fin de comunicar presuntos casos de fraude, colusión y corrupción por parte de los funcionarios y servidores de la Entidad, así como los proveedores y demás actores que participan en el proceso de contratación.

De igual forma, deben poner en conocimiento de la Secretaría Técnica de la Comisión de Defensa de la Libre Competencia del INDECOPI los indicios de conductas anticompetitivas que se presenten durante el proceso de contratación, en los términos del Decreto Legislativo N° 1034, "Ley de Represión de Conductas Anticompetitivas", o norma que la sustituya, así como las demás normas de la materia.

La Entidad y todo proveedor que se someta a las presentes Bases, sea como participante, postor y/o contratista del proceso de contratación deben permitir a la Secretaría Técnica de la Comisión de Defensa de la Libre Competencia del INDECOPI el acceso a la información que sea requerida, prestar testimonio o absolución de posiciones que se requieran, entre otras formas de colaboración.

CAPÍTULO I

1. DISPOSICIONES GENERALES Y SERVICIO A CONTRATAR

1.1 OBJETO DEL PROCESO DE CONCURSO DE MERITOS

El Banco de la Nación convoca a un concurso de méritos para contratar una empresa especializada, para que preste el Servicio de implementación de nueva plataforma bancaria para canales digitales banca móvil y banca por internet del Banco de la Nación.

El presente proyecto de la nueva plataforma de los canales digitales del Banco de la Nación tiene como alcance principal la modernización y optimización de la Banca Móvil y la Banca por Internet. Se busca mejorar la experiencia del usuario, asegurar el consumo eficiente de los recursos de Nube (procesamiento, seguridad, ejecución de APIs, entre otros componentes) y cumplir con las demandas tecnológicas actuales del mercado. Para alcanzar este objetivo, se contempla la incorporación de diversos mecanismos tecnológicos disponibles en el mercado actual. Estos elementos respaldarán los volúmenes de transacciones financieras y no financieras que se llevarán a cabo a través de estos canales digitales.

1.2 ALCANCES DEL REQUERIMIENTO

El alcance de la prestación está definido en el **Anexo N° 1** - Términos de Referencia, de la presente bases.

1.3 CONDICIONES DEL SERVICIO

1.3.1 VALOR REFERENCIAL

El valor referencial del presente Concurso de Méritos es de **S/ 30,530,187.96 (Treinta millones quinientos treinta mil ciento ochenta y siete con 96/100 Soles)**, el cual incluye todos los tributos, los costos laborales conforme a la legislación vigente; así como, cualquier otro concepto que pueda tener incidencia sobre el costo del servicio a contratar.

1.3.2 SISTEMA DE CONTRATACIÓN

El sistema de contratación para el servicio de la "Implementación de la nueva plataforma bancaria para los canales digitales Banca Móvil y Banca por Internet del Banco de la Nación" es un **Esquema Mixto de Suma Alzada y Precios Unitarios**.
De acuerdo con el siguiente detalle:

Sistema de Contratación para la Implementación del Proyecto

Concepto	Descripción	Tipo de Esquema mixto
Diseño, Desarrollo e Implementación de la Solución (21.1)	Incluye diseño de interfaz, desarrollo e implementación de las funcionalidades de la Banca Móvil y Banca por Internet descritas en el numeral 7. Alcance y Descripción del Servicio y en el numeral 13. Desarrollo de APIs	**Suma alzada**

Implementación de la Infraestructura (21.2.b.1)	Despliegue base para los ambientes	**Suma alzada**
	Despliegue del ambiente de desarrollo (DEV)	**Suma alzada**
	Despliegue del ambiente de Calidad (QA)	**Suma alzada**
	Despliegue del ambiente de Producción (PRD)	**Suma alzada**
Implementación del Ambiente de Seguridad (21.2.b.2.)	Servicio de implementación Plataforma de protección para aplicaciones CNAPP	**Suma alzada**
	Servicio Implementación Firewall	**Suma alzada**
	Servicio Implementación SaaS de Seguridad para los servicios WAF, ataques volumétricos de denegación de servicio y servicio de seguridad de API discovery	**Suma alzada**
	Servicio Implementación para el Servicio de Detección Avanzada para ataques de Bots Automatizados	**Suma alzada**
Servicio de Soporte Técnico (21.2.b.4.)	Soporte técnico para la atención y resolución de todos los problemas que se presenten con la solución propuesta	**Suma alzada**
Servicio de Asistencia para Alcanzar la Mejora Continua de la Solución (21.2.b.4.)	Tendrá una duración de 90 días calendarios bajo la modalidad de bolsa de trabajo que considera 600 horas mensuales (total del servicio 1,800 horas), terminado el periodo de 90 días, el servicio tendrá la modalidad bajo demanda durante el tiempo de ejecución del contrato.	**Precios unitarios**
	Despues de los 90 días calendarios, el servicio tendrá la modalidad bajo demanda durante el tiempo de ejecución del contrato.	**Precios unitarios**

Sistema de Contratación para los componentes del Proyecto

Las especificaciones de capacidades siguientes deberán cotizarse para el consumo de Banco de la nación, a no ser que estos servicios de Nube se entreguen en su totalidad en modalidad SaaS 100% gestionada por el contratista a costo fijo, ya sea para los servicios compartidos, los componentes a demanda y para los ambientes de Producción, Certificación (QA) y Desarrollo (Dev).

Ítem	Componente	Tipo de Esquema mixto
10.1. Servicios Compartidos		
1	Componentes del Servicio	**Precio unitario**
2	Servicio de NAT Horas	**Precio unitario**
3	Conexión VPN Site to Site	**Precio unitario**
4	Conexión Cliente VPN	**Precio unitario**
5	Conector de redes en múltiples zonas	**Precio unitario**
6	Servicio de transferencia de datos	**Precio unitario**
7	Kit de desarrollo de software en la nube	**Precio unitario**
8	Servicio de entrega continua	**Precio unitario**
9	Repositorio de paquetes de software	**Precio unitario**
10	Servicio de construcción e integración continua con Sistema operativo Linux.	**Precio unitario**
11	Recurso de cómputo con las siguientes características: 8 vCPU y 16 GB Memoria	**Precio unitario**
12	Registro de contenedores	**Precio unitario**

13	Servicio de autenticación Web/móvil	**Precio unitario**
14	Servicio de logs de la consola en nube	**Precio unitario**
10.2. Ambiente de Producción		
1	Componentes del Servicio	**Precio unitario**
2	Servicio de base de datos relacional compatible con PostgreSQL en alta disponibilidad (Primario/Respaldo) en multizona	**Precio unitario**
3	Cada característica puede consumirse de manera independiente	**Precio unitario**
4	Servicio de base de datos de documentos compatible con (mongoDB) Cada característica puede consumirse de manera independiente 2 Instancias, una por Zona de disponibilidad	**Precio unitario**
5	Servicio de administración y despliegue de APIs	**Precio unitario**
6	Balanceador de carga de red	**Precio unitario**
7	Servicio de contenedores basado en Kubernetes	**Precio unitario**
8	Servicio de máquinas virtuales de cómputo para kubernetes con Sistema operativo Linux	**Precio unitario**
9	Servicio de CDN	**Precio unitario**
10	Servicio de gestión de claves criptográficas	**Precio unitario**
11	Servicio de almacenamiento de secretos	**Precio unitario**
12	Servicio de almacenamiento de objetos	**Precio unitario**
13	Servicio de monitoreo y observabilidad	**Precio unitario**
14	SFTP	**Precio unitario**
15	Servicio de ejecución de Funciones sin servidor	**Precio unitario**
10.3. Ambiente de Certificación (QA)		
1	Componentes del Servicio	**Precio unitario**
2	Servicio de base de datos relacional compatible con PostgreSQL en alta disponibilidad (Primario/Respaldo) en multizona	**Precio unitario**
3	Servicio de base de datos de documentos compatible con (mongoDB) Cada característica puede consumirse de manera independiente 2 Instancias, una por Zona de disponibilidad	**Precio unitario**
4	Servicio de administración y despliegue de APIs	**Precio unitario**
5	Balanceador de carga de de aplicación	**Precio unitario**
6	Servicio de contenedores basado en Kubernetes	**Precio unitario**
7	Servicio de máquinas virtuales de cómputo con Sistema operativo Linux	**Precio unitario**
8	Servicio de CDN	**Precio unitario**
9	Servicio de gestión de claves criptográficas	**Precio unitario**
10	Servicio de almacenamiento de secretos	**Precio unitario**
11	Servicio de almacenamiento de objetos	**Precio unitario**
12	Servicio de monitoreo y observabilidad	**Precio unitario**
13	SFTP	**Precio unitario**
14	Servicio de ejecución de Funciones sin servidor	**Precio unitario**
10.4. Ambiente Desarrollo (DEV)		
1	Componentes del Servicio	**Precio unitario**
2	Servicio de base de datos relacional compatible con PostgreSQL	**Precio unitario**
3	Servicio de base de datos de documentos compatible con (mongoDB) Servicio de administración y despliegue de APIs	**Precio unitario**
4	Balanceador de carga de aplicación	**Precio unitario**
5	Servicio de contenedores basado en Kubernetes	**Precio unitario**
6	Servicio de máquinas virtuales de cómputo con Sistema operativo Linux	**Precio unitario**
7	Servicio de CDN	**Precio unitario**
8	Servicio de gestión de claves criptográficas	**Precio unitario**
9	Servicio de almacenamiento de secretos	**Precio unitario**
10	Servicio de almacenamiento de objetos	**Precio unitario**

11	Servicio de monitoreo y observabilidad	**Precio unitario**
12	SFTP	**Precio unitario**
13	Servicio de ejecución de Funciones sin servidor	**Precio unitario**
10.5. Componentes a Demanda		
1	Servicio de base de datos relacional (HA)	**Precio unitario**
2	Servicio de base de datos de documentos	**Precio unitario**
3	Servicio de máquinas virtuales de cómputo para kubernetes con Sistema operativo Linux	**Precio unitario**
4	Direct Connet hosteado	**Precio unitario**
11.8. Especificaciones de Capacidades de los Servicios de Seguridad		
1	Componentes del Servicio	**Suma alzada**
2	Consola SaaS de Seguridad para los servicios WAF, ataques volumétricos de denegación de servicio y servicio de seguridad de APIs.	**Suma alzada**
3	Plataforma de protección nativa de nube para aplicaciones (CNAPP)	**Suma alzada**
4	Servicio de Next Generation Firewall (NGFW)	**Suma alzada**

Sistema de Contratación para la integración con Cuenta DNI

Concepto	Escenarios Opcionales	Tipo de Esquema mixto
Cuenta DNI	**Escenario 1:** El contratista deberá realizar el desarrollo correspondiente a fin de enlazar los servicios del APP con los recursos de nube donde se encuentra alojado Cuenta DNI. Se coordinará con el proveedor los accesos correspondientes y las pruebas necesarias.	**Suma alzada**
	Escenario 2: La Cuenta DNI será considerada como una Cuenta BN y el Contratista deberá realizar el desarrollo a fin de dar el mismo tratamiento que a las demás cuentas que se encuentran registradas en el Core Bancario (Mainframe).	**Suma alzada**

Sin embargo, para el concepto cantidad de integraciones y/o incremento de requerimientos de negocio en exceso, corresponderá el sistema de contratación a precios unitarios a través de una cantidad de horas (bolsa de horas) durante la vigencia del contrato, la cual solo se activará a petición del Banco de la Nación y no se cobrará en caso no se use.

1.3.3 LUGAR Y PLAZO DE LA PRESTACION DEL SERVICIO

a) Lugar

El servicio se ofrecerá en la sede principal del Banco de la Nación, ubicada en la Av. Javier Prado Este 2499, San Borja. El desarrollo del proyecto podrá ser realizado de forma remota. No obstante, el Banco tendrá la opción de solicitar presencialidad en caso lo considere necesario. Las actividades y las reuniones de trabajo con el personal del Banco se llevarán a cabo a través de la Plataforma Virtual del Banco o en la mencionada oficina principal.

b) Plazo de Ejecución de la prestación del servicio

Desarrollo de la Aplicación

El plazo de contratación del servicio de la nueva plataforma bancaria para los canales digitales Banca Móvil y Banca por Internet del Banco de la Nación será de **420 días** calendarios. El inicio de la contraprestación del servicio será a partir del día siguiente de aprobado el **Plan de Trabajo**.

Servicios de Nube

El plazo de contratación de lo servicio de nube para la nueva plataforma bancaria para los canales digitales Banca Móvil y Banca por Internet del Banco de la Nación será de **36 meses** como máximo. El inicio de la contraprestación del servicio será a partir del día siguiente de aprobado el **Plan de Trabajo**.

Servicio de Asistencia para Alcanzar la Mejora Continua de la Solución

El servicio de Mejora Continua (ver numeral 33. Mejora Continua del Servicio) tendrá una duración de **90 días calendarios** bajo la modalidad de bolsa de trabajo que considera 600 horas mensuales (total del servicio 1,800 horas), terminado el periodo de 90 días, el servicio tendrá la modalidad a demanda durante el tiempo de ejecución del contrato.

El inicio del servicio de Mejora Continua empezará al día siguiente de la suscripción del Acta de Conformidad correspondiente al MVP 4.

1.3.4 FORMA DE PAGO

El pago se realizará en la moneda nacional (soles) por la prestación efectiva del servicio instalado. En el caso de ofertas presentadas en moneda extranjera, el pago se ajustará al tipo de cambio Venta Promedio Ponderado, publicado por la Superintendencia de Banca y Seguros (SBS) en la fecha del registro contable de los pagos. Este proceso se llevará a cabo luego de recibir de manera formal y completa toda la documentación correspondiente.

El Contratista debe incluir en su propuesta los rangos de uso mensual correspondientes a los distintos componentes de la solución. Esto implica detallar la capacidad de la solución para manejar distintos volúmenes de transacciones, especificando claramente los límites de uso para cada componente, como el almacenamiento en la nube, el procesamiento de datos, la transferencia de datos y otros servicios relacionados. Es fundamental que los rangos de uso sean adecuados, por precio unitario según el rango mensual y estén alineados con las necesidades del proyecto, permitiendo una planificación precisa y garantizando la escalabilidad de la solución a lo largo del tiempo. En este contexto, el Contratista deberá considerar el Anexo N° 6 de los Términos de Referencia para la presentación de sus rangos de uso propuestos, el cual deberá ser incluido en su propuesta económica.

El contratista deberá consolidar la documentación correspondiente según el siguiente cuadro:

Tabla 1: Cuadro de Aprobación por Área Responsable

Gerencia o Subgerencia Responsable	Referencia
Gerencia de Banca Digital (Subgerencia Innovación Digital)	Numeral 21.1. Diseño, Desarrollo e Implementación de la Solución
Gerencia de Tecnologías de la Información	Numeral 21.2. Servicios de alojamiento, procesamiento y seguridad de la Solución
Gerencia de Banca Digital (Subgerencia Innovación Digital)	Numeral 21.3 Componente opcional – Cuenta DNI
Gerencia de Banca Digital (Subgerencia Innovación Digital)	Numeral 21.4 19.3. Servicio de Asistencia para Alcanzar la Mejora Continua de la Solución

La documentación necesaria para los pagos por parte del Contratista deberá ser enviada en formato físico a la sede central del Banco de la Nación, ubicada en la calle Arqueología N° 120, San Borja, Lima, durante el horario de oficina.

Diseño, Desarrollo e Implementación de la Solución

El pago se realizará tras la emisión del Acta de Conformidad correspondiente a cada entregable definido.

El Banco realizará los pagos al Contratista en diez (10) partes, según se especifica en el cuadro de plazos de los entregables y porcentajes de pago correspondiente al desarrollo de la solución. Estos pagos estarán condicionados al cumplimiento del envío de los documentos establecidos en el numeral 16 de Entregables.

A fin de proceder con el pago correspondiente al entregables, el Contratista deberá remitir al Banco de la Nación la siguiente documentación:

a. Carta simple dirigida al Subgerente de Compras de la Gerencia de Administración y Logística.
b. Comprobante de pago
c. Acta de Conformidad original de la Subgerencia de Innovación Digital como área usuaria
d. Informe de la Subgerencia de Innovación Digital como área usuaria y sus anexos, en caso de que los haya.

El Contratista estará encargado de desarrollar e implementar los APIs necesarios para el proyecto (ver numeral 13. Desarrollo de APIs). El costo de estos APIs debe estar incluido en los costos totales de desarrollo e implementación de la nueva plataforma de los Canales Digitales del Banco de Nación y no será sujeto a pagos diferenciados.

Para reflejar la importancia y el peso de las actividades para cada MVP, se asignará un porcentaje de la facturación total de desarrollo de la solución, basado en la complejidad y el valor de las funcionalidades a desarrollar.

Los pagos se realizarán en base a los entregables propuestos, según el siguiente cuadro:

Tabla 2: Forma de Pago para el Desarrollo e Implementación del Producto.

N°	Entregable	Referencia	Días calendarios del plazo de entregables, contados desde aprobación del Plan de Trabajo	Porcentaje de Facturación por Desarrollo de Solución
1	Análisis funcional	7. ALCANCE Y DESCRIPCIÓN DEL SERVICIO	60	5.00%
2	Diseño UX / UI	7. ALCANCE Y DESCRIPCIÓN DEL SERVICIO 7.1. Descripción y condiciones del servicio, literal "c".	75	5.00%
3	Codificación y Pentesting MVP 1	7.2. Enrolamiento al canal digital 7.3. Enrolamiento a la Cuenta DNI 7.4 Afiliación a la Clave Dinámica Digital (CDD) 7.5 Gestión de Claves Centralizadas 7.6 Recuperación de la contraseña de Internet 7.7 Primer Inicio de Sesión 7.8 Inicio de Sesión del Cliente Recurrente 7.9 Factores de Autenticación y Seguridad del Cliente	165	11.00%

		7.10 Consultas de Productos, Saldos y Movimientos 7.11 Transferencias Bancarias 7.12 Retiro sin tarjeta y por agentes corresponsales 7.13 Módulo de Seguridad 7.14 Configuración de Multidioma (lenguas originarias)		
4	Despliegue en Producción MVP 1	-	180	14.50%
5	Codificación y Pentesting MVP 2	7.15 Pago de Servicios y pago a empresas 7.16 Recargas móviles 7.11 Transferencias Bancarias (Diferidas) 7.17 Actualización de Datos Personales 7.18 Operaciones Favoritas 7.19 Giros Nacionales 7.20 Bloqueo de Tarjetas de Débito o de Crédito	255	9.00%
6	Despliegue en Producción MVP 2	-	270	13.50%
7	Codificación y Pentesting MVP 3	7.21 Pago de Tarjeta de Crédito 7.22 Créditos Digitales 7.23 Consulta de Estado de Cuenta 7.24 Ubicación de Agencias, Cajeros y Agentes 7.25 Configuración de los atributos de Cuentas y Tarjetas de los clientes	345	9.00%
8	Despliegue en Producción MVP 3	-	360	13.50%
9	Codificación y Pentesting MVP 4	7.26 Módulo de Administración 7.27 Pago de Tasas	405	9.00%
10	Despliegue en Producción MVP 4	-	420	10.50%
			Total	**100.00%**

El proveedor ganador de la buena pro deberá cumplir con los porcentajes y plazos establecidos en la Tabla 16 Forma de Pago para el Desarrollo e Implementación del Producto para los entregables 1 (Análisis Funcional) y 2 (Diseño UX/UI), independientemente de si opta por ejecutar estas actividades en su totalidad al inicio del proyecto o de forma parcial y proporcional en cada MVP (Producto Mínimo Viable).

Servicios de Alojamiento, Procesamiento y Seguridad de la Solución

Los pagos se efectuarán por prestaciones completadas de acuerdo a las tarifas establecidas para cada rango según modalidad de validación y los consumos mensuales de prestaciones efectivas y debidamente acreditadas según los requisitos solicitados.

a. Forma y Plazo para el Pago del Servicio de Alojamiento, Procesamiento y Seguridad

Los pagos se realizarán en base a la implementación de los hitos propuestos, según el siguiente cuadro:

Tabla 3: Forma de pago para los costos fijos el Servicio de Alojamiento, Procesamiento y Seguridad de la Solución

Implementación del servicio de nube	Hitos	Referencias	Plazo máximo de entrega (en días calendarios)	% de pago
Para el pago de la implementación de la infraestructura	Despliegue Base para los Ambientes	21.2 Servicios de Alojamiento, Procesamiento y Seguridad de la Solución, literal b.1 Para el Pago de la Implementación de la Infraestructura, literal b.1.1 Despliegue Base para los Ambientes	55 días posteriores a la fecha de la firma del acta de conformidad del plan de trabajo.	25% del costo de implementación de la infraestructura
	Despliegue del Ambiente de Desarrollo (DEV)	21.2 Servicios de Alojamiento, Procesamiento y Seguridad de la Solución, literal b.1 Para el Pago de la Implementación de la Infraestructura, b.1.2 Despliegue del Ambiente de Desarrollo (DEV)	35 días posteriores a la fecha de aprobación del informe técnico de Despliegue base para los ambientes.	25% del costo de implementación de la infraestructura
	Despliegue del Ambiente de Calidad (QA)	21.2 Servicios de Alojamiento, Procesamiento y Seguridad de la Solución, literal b.1 Para el Pago de la Implementación de la Infraestructura, b.1.3 Despliegue del Ambiente de Calidad (QA)	35 días posteriores a la fecha de aprobación del informe técnico de Despliegue del ambiente de desarrollo.	25% del costo de implementación de la infraestructura
	Despliegue del Ambiente de Producción	21.2 Servicios de Alojamiento, Procesamiento y	35 días posteriores a la fecha de aprobación del informe técnico de	25% del costo de implementación de la infraestructura

	(PRD)	Seguridad de la Solución, literal b.1 Para el Pago de la Implementación de la Infraestructura, b.1.4 Despliegue del Ambiente de Producción (PRD)	Despliegue del ambiente de calidad.	
Para el pago de la implementación del ambiente de seguridad	Servicio de Implementación Plataforma de Protección para Aplicaciones CNAPP	21.2 Servicios de Alojamiento, Procesamiento y Seguridad de la Solución, literal b.2 Para el Pago de la Implementación del Ambiente de Seguridad, b.2.1 Servicio de Implementación Plataforma de Protección para Aplicaciones CNAPP	60 días posteriores a la fecha del informe de aprobación del ambiente de desarrollo (DEV).	25% del costo de implementación del ambiente de seguridad
	Servicio Implementación Firewall	21.2 Servicios de Alojamiento, Procesamiento y Seguridad de la Solución, literal b.2 Para el Pago de la Implementación del Ambiente de Seguridad, b.2.2 Servicio Implementación Firewall		25% del costo de implementación del ambiente de seguridad
	Servicio Implementación SaaS de Seguridad para los servicios WAF, ataques volumétricos de denegación de servicio y servicio de seguridad de API Discovery	21.2 Servicios de Alojamiento, Procesamiento y Seguridad de la Solución, literal b.2 Para el Pago de la Implementación del Ambiente de Seguridad, b.2.3 Servicio Implementación SaaS de Seguridad para los Servicios WAF, Ataques Volumétricos de Denegación de Servicio y Servicio de Seguridad de		25% del costo de implementación del ambiente de seguridad

		API Discovery		
	Servicio Implementación para el Servicio de Detección Avanzada para ataques de Bots Automatizados	21.2 Servicios de Alojamiento, Procesamiento y Seguridad de la Solución, literal b.2 Para el Pago de la Implementación del Ambiente de Seguridad, b.2.4 Servicio Implementación para el Servicio de Detección Avanzada para Ataques de Bots Automatizados		25% del costo de implementación del ambiente de seguridad

Tabla 4: Forma de pago para los costos variables el Servicio de Alojamiento, Procesamiento y Seguridad de la Solución

Implementación del servicio de nube	**Hitos**	**Referencias**	**Plazo máximo de entrega (en días calendarios)**
Para el pago mensual* por uso de infraestructura y ambiente de seguridad	Pago mensual de infraestructura	21.2 Servicios de Alojamiento, Procesamiento y Seguridad de la Solución, literal b.3 Para el Pago Mensual por Uso de Infraestructura y Ambiente de Seguridad, b.3.1 Pago Mensual de Infraestructura	El pago por el uso de los componentes de infraestructura se realizará al final de cada mes según los consumos realizados por cada uno de estos componentes especificados en las Tablas de Capacidades. (considerar DEV, QA, PRD, seguridad y compartidos).
	Pago mensual del servicio de seguridad	21.2 Servicios de Alojamiento, Procesamiento y Seguridad de la Solución, literal b.3 Para el Pago Mensual por Uso de Infraestructura y Ambiente de Seguridad, b.3.2 Pago Mensual del Servicio de Seguridad	
Para el pago del soporte técnico	Pago mensual por soporte técnico	21.2 Servicios de Alojamiento, Procesamiento y Seguridad de la Solución, literal b.4 Para el Pago del Soporte Técnico, b.4.1 Pago Mensual de Soporte Técnico	El pago por el soporte y mantenimiento de la infraestructura y seguridad se realizará al final de cada mes, hasta el final del contrato, iniciándose este soporte y mantenimiento al finalizar la implementación del ambiente de producción

*El pago se realizará de acuerdo con el consumo efectivo mensual y las tarifas por rangos y componentes del servicio que presenten los postores en su oferta económica.

b.1 Para el Pago de la Implementación de la Infraestructura

La documentación para los pagos por parte del Contratista será remitida en formato físico a la

sede central del Banco de la Nación, sitio en calle Arqueología N° 120, San Borja, Lima, en horario de oficina.

b.1.1 Despliegue Base para los Ambientes

El Contratista deberá entregar un informe que evidencie el despliegue base de servicios y configuraciones para los ambientes a implementar (Desarrollo, Certificación y Producción), así como la descripción de cada uno de los componentes a ser desplegados en esta etapa y si hubiera alguna descripción adicional también debe ser informada.

El Banco revisará el informe como máximo en 5 días calendario como máximo y si hubiera alguna observación se le indicará al Contratista a través de correo electrónico al líder de proyecto del Contratista para la subsanación respectiva, para lo cual el Contratista tendrá 5 días calendarios adicionales como máximo para la subsanación. Una vez concluida la revisión por parte del Banco se emitirá un informe técnico y posteriormente el acta de conformidad para el pago.

Los responsables de la aprobación del informe técnico serán las áreas siguientes:

- Subgerencia de Construcción
- Subgerencia de Arquitectura
- Subgerencia de Producción
- Oficina de Seguridad informática

El Banco comunicara al Contratista la fecha de aprobación del informe técnico para que al día siguiente inicie la implementación del ambiente de desarrollo.

El responsable del acta de conformidad será la Subgerencia de Innovación Digital de la Gerencia Banca Digital.

Los documentos a entregar por parte del Contratista para el pago serán:

- Carta simple dirigida al subgerente de compras de la gerencia de administración y logística
- Acta de conformidad suscrita por la Subgerencia de Innovación Digital de la Gerencia Banca Digital.
- Comprobante de pago.
- Informe técnico por parte de la Gerencia de TI especificado anteriormente.
- Copia del contrato.

b.1.2 Despliegue del Ambiente de Desarrollo (DEV)

El Contratista deberá entregar un informe que evidencie el despliegue de los componentes necesarios para el uso del ambiente de desarrollo, así como la habilitación de servicios y configuraciones necesarias, así como la descripción de cada uno de los componentes y servicios desplegados en esta etapa y si hubiera alguna descripción adicional también debe ser informada.

El Banco revisará el informe como máximo en 5 días calendario y si hubiera alguna observación se le indicará al Contratista a través de correo electrónico al líder de proyecto del Contratista para la subsanación respectiva, para lo cual el Contratista tendrá 5 días calendarios adicionales como máximo para la subsanación. Una vez concluida la revisión por parte del Banco se emitirá un informe técnico y posteriormente el acta de conformidad para el pago.

Los responsables de la aprobación del informe técnico serán las áreas siguientes es:

- Subgerencia de Construcción
- Subgerencia de Arquitectura

- Subgerencia de Producción
- Oficina de Seguridad Informática

El Banco comunicara al Contratista la fecha de aprobación del informe técnico para que al día siguiente inicie la implementación del ambiente de Calidad.
El responsable del acta de conformidad será la Subgerencia de Innovación Digital de la Gerencia Banca Digital.

Los documentos a entregar por parte del Contratista para el pago serán:

- Carta simple dirigida al subgerente de compras de la gerencia de administración y logística
- Acta de conformidad suscrita por la Subgerencia de Innovación Digital de la Gerencia Banca Digital.
- Comprobante de pago.
- Informe técnico por parte de la Gerencia de TI especificado anteriormente.
- Copia del contrato.

b.1.3 Despliegue del Ambiente de Calidad (QA)

El Contratista deberá entregar un informe que evidencie el despliegue de los componentes necesarios para el uso del ambiente de calidad, así como la habilitación de servicios y configuraciones necesarias, así como la descripción de cada uno de los componentes y servicios desplegados en esta etapa y si hubiera alguna descripción adicional también debe ser informada.
El Banco revisará el informe como máximo en 5 días calendario y si hubiera alguna observación se le indicará al Contratista a través de correo electrónico al líder de proyecto del Contratista para la subsanación respectiva, para lo cual el Contratista tendrá 5 días calendarios adicionales como máximo para la subsanación. Una vez concluida la revisión por parte del Banco se emitirá un informe técnico y posteriormente el acta de conformidad para el pago.
Los responsables de la aprobación del informe técnico serán las áreas siguientes es:

- Subgerencia de Construcción
- Subgerencia de Arquitectura
- Subgerencia de Producción
- Oficina de Seguridad Informática

El Banco comunicara al Contratista la fecha de aprobación del informe técnico para que al día siguiente inicie la implementación del ambiente de Producción.
El responsable del acta de conformidad será la Subgerencia de Innovación Digital de la Gerencia Banca Digital.

Los documentos a entregar por parte del Contratista para el pago serán:

- Carta simple dirigida al subgerente de compras de la gerencia de administración y logística
- Acta de conformidad suscrita por la Subgerencia de Innovación Digital de la Gerencia Banca Digital.
- Comprobante de pago.
- Informe técnico por parte de la Gerencia de TI especificado anteriormente.
- Copia del contrato.

b.1.4 Despliegue del Ambiente de Producción (PRD)

El Contratista deberá entregar un informe que evidencie el despliegue de los componentes necesarios para el uso del ambiente de producción, así como la

habilitación de servicios y configuraciones necesarias, así como la descripción de cada uno de los componentes y servicios desplegados en esta etapa y si hubiera alguna descripción adicional también debe ser informada.

El Banco revisará el informe como máximo en 5 días calendario y si hubiera alguna observación se le indicará al Contratista a través de correo electrónico al líder de proyecto del Contratista para la subsanación respectiva, para lo cual el Contratista tendrá 5 días calendarios adicionales como máximo para la subsanación. Una vez concluida la revisión por parte del Banco se emitirá un informe técnico y posteriormente el acta de conformidad para el pago.

Los responsables de la aprobación del informe técnico serán las áreas siguientes es:

- Subgerencia de Construcción
- Subgerencia de Arquitectura
- Subgerencia de Producción
- Oficina de Seguridad Informática

El responsable del acta de conformidad será la Subgerencia de Innovación Digital de la Gerencia Banca Digital.

Los documentos a entregar por parte del Contratista para el pago serán:

- Carta simple dirigida al subgerente de compras de la gerencia de administración y logística
- Acta de conformidad suscrita por la Subgerencia de Innovación Digital de la Gerencia Banca Digital.
- Comprobante de pago.
- Informe técnico por parte de la Gerencia de TI especificado anteriormente.
- Copia del contrato.

b.2 Para el Pago de la Implementación del Ambiente de Seguridad

b.2.1 Servicio de Implementación Plataforma de Protección para Aplicaciones CNAPP

El Contratista deberá entregar un informe sobre el despliegue de los componentes necesarios para el uso de la plataforma de protección para aplicaciones (CNAPP), así como la habilitación de servicios y configuraciones necesarias, así como la descripción de cada uno de los componentes y servicios desplegados en esta etapa y si hubiera alguna descripción adicional también debe ser informada.

El Banco revisará el informe como máximo en 5 días calendario y si hubiera alguna observación se le indicará al Contratista a través de correo electrónico al líder de proyecto del Contratista para la subsanación respectiva, para lo cual el Contratista tendrá 5 días calendarios adicionales como máximo para la subsanación. Una vez concluida la revisión por parte del Banco se emitirá un informe técnico y posteriormente el acta de conformidad para el pago.

Los responsables de la aprobación del informe técnico serán las áreas siguientes es:

- Subgerencia de Construcción
- Subgerencia de Arquitectura
- Subgerencia de Producción
- Oficina de Seguridad Informática

El responsable del acta de conformidad será la Subgerencia de Innovación Digital de la Gerencia Banca Digital.

Los documentos a entregar por parte del Contratista para el pago serán:

- Carta simple dirigida al subgerente de compras de la gerencia de administración y logística
- Acta de conformidad suscrita por la Subgerencia de Innovación Digital de la Gerencia Banca Digital.
- Comprobante de pago.
- Informe técnico por parte de la Gerencia de TI especificado anteriormente.
- Copia del contrato.

b.2.2 Servicio Implementación Firewall

El Contratista deberá entregar un informe sobre el despliegue de los componentes necesarios para el uso de los servicios de Firewall, así como la habilitación de servicios y configuraciones necesarias, así como la descripción de cada uno de los componentes y servicios desplegados en esta etapa y si hubiera alguna descripción adicional también debe ser informada.

El Banco revisará el informe como máximo en 5 días calendario y si hubiera alguna observación se le indicará al Contratista a través de correo electrónico al líder de proyecto del Contratista para la subsanación respectiva, para lo cual el Contratista tendrá 5 días calendarios adicionales como máximo para la subsanación. Una vez concluida la revisión por parte del Banco se emitirá un informe técnico y posteriormente el acta de conformidad para el pago.

Los responsables de la aprobación del informe técnico serán las áreas siguientes es:

- Subgerencia de Construcción
- Subgerencia de Arquitectura
- Subgerencia de Producción
- Oficina de Seguridad Informática

El responsable del acta de conformidad será la Subgerencia de Innovación Digital de la Gerencia Banca Digital.

Los documentos a entregar por parte del Contratista para el pago serán:

- Carta simple dirigida al subgerente de compras de la gerencia de administración y logística
- Acta de conformidad suscrita por la Subgerencia de Innovación Digital de la Gerencia Banca Digital.
- Comprobante de pago.
- Informe técnico por parte de la Gerencia de TI especificado anteriormente.
- Copia del contrato.

b.2.3 Servicio Implementación SaaS de Seguridad para los Servicios WAF, Ataques Volumétricos de Denegación de Servicio y Servicio de Seguridad de API Discovery

El Contratista deberá entregar un informe sobre el despliegue de los componentes necesarios para el uso de los Servicio Implementación SaaS de Seguridad para los servicios WAF, ataques volumétricos de denegación de servicio y servicio de seguridad de API Discovery, así como la habilitación de servicios y configuraciones necesarias, así como la descripción de cada uno de los componentes y servicios desplegados en esta etapa y si hubiera alguna descripción adicional también debe ser informada.

El Banco revisará el informe como máximo en 5 días calendario y si hubiera alguna observación se le indicará al Contratista a través de correo electrónico al líder de proyecto del Contratista para la subsanación respectiva, para lo cual el Contratista

tendrá 5 días calendarios adicionales como máximo para la subsanación. Una vez concluida la revisión por parte del Banco se emitirá un informe técnico y posteriormente el acta de conformidad para el pago.

Los responsables de la aprobación del informe técnico serán las áreas siguientes es:

- Subgerencia de Construcción
- Subgerencia de Arquitectura
- Subgerencia de Producción
- Oficina de Seguridad Informática

El responsable del acta de conformidad será la Subgerencia de Innovación Digital de la Gerencia Banca Digital.

Los documentos a entregar por parte del Contratista para el pago serán:

- Carta simple dirigida al subgerente de compras de la gerencia de administración y logística
- Acta de conformidad suscrita por la Subgerencia de Innovación Digital de la Gerencia Banca Digital.
- Comprobante de pago.
- Informe técnico por parte de la Gerencia de TI especificado anteriormente.
- Copia del contrato.

b.2.4 Servicio Implementación para el Servicio de Detección Avanzada para Ataques de Bots Automatizados

El Contratista deberá entregar un informe sobre despliegue de los componentes necesarios para el uso de los Servicio Implementación para el Servicio de Detección Avanzada para ataques de Bots Automatizados, así como la habilitación de servicios y configuraciones necesarias, así como la descripción de cada uno de los componentes y servicios desplegados en esta etapa y si hubiera alguna descripción adicional también debe ser informada.

El Banco revisará el informe como máximo en 5 días calendario y si hubiera alguna observación se le indicará al Contratista a través de correo electrónico al líder de proyecto del Contratista para la subsanación respectiva, para lo cual el Contratista tendrá 5 días calendarios adicionales como máximo para la subsanación. Una vez concluida la revisión por parte del Banco se emitirá un informe técnico y posteriormente el acta de conformidad para el pago.

Los responsables de la aprobación del informe técnico serán las áreas siguientes es:

- Subgerencia de Construcción
- Subgerencia de Arquitectura
- Subgerencia de Producción
- Oficina de Seguridad Informática

El responsable del acta de conformidad será la Subgerencia de Innovación Digital de la Gerencia Banca Digital.

Los documentos a entregar por parte del Contratista para el pago serán:

- Carta simple dirigida al subgerente de compras de la gerencia de administración y logística
- Acta de conformidad suscrita por la Subgerencia de Innovación Digital de la Gerencia Banca Digital.
- Comprobante de pago.
- Informe técnico por parte de la Gerencia de TI especificado anteriormente.
- Copia del contrato

b.3 Para el Pago Mensual por Uso de Infraestructura y Ambiente de Seguridad

b.3.1 Pago Mensual de Infraestructura

El pago por el uso de los componentes de infraestructura se realizará al final de cada mes según los consumos realizados por cada uno de estos componentes especificados en las Tablas de Capacidades. (considerar dev, qa, prd y compartidos).

En situaciones donde el servicio se inicie en un día que no coincida con el comienzo de un mes calendario, se aplicara el prorrateo. El prorrateo consistirá en calcular la proporción del servicio utilizado desde la fecha de inicio hasta el final del mes en curso y facturar únicamente por ese período inicial de manera proporcional.

El Contratista emitirá un informe a cada fin de mes indicando los consumos realizados por cada uno de los componentes, reportes de monitoreo, Incidencias generadas, así como las soluciones realizadas, además de recomendaciones de mejora de ser el caso.

El Banco revisará el informe como máximo en 5 días calendario y si hubiera alguna observación se le indicará al Contratista a través de correo electrónico al líder de proyecto del Contratista para la subsanación respectiva, para lo cual el Contratista tendrá 5 días calendarios adicionales como máximo para la subsanación. Una vez concluida la revisión por parte del Banco se emitirá un informe técnico y posteriormente el acta de conformidad para el pago.

Los responsables de la aprobación del informe técnico serán las áreas siguientes es:

- Subgerencia de Construcción
- Subgerencia de Producción

El responsable del acta de conformidad será la Subgerencia de Innovación Digital de la Gerencia Banca Digital.

Los documentos a entregar por parte del Contratista para el pago serán:

- Carta simple dirigida al subgerente de compras de la gerencia de administración y logística
- Acta de conformidad suscrita por la Subgerencia de Innovación Digital de la Gerencia Banca Digital.
- Comprobante de pago.
- Informe técnico por parte de la Gerencia de TI especificado anteriormente.
- Copia del contrato.

b.3.2 Pago Mensual del Servicio de Seguridad

El pago por el uso de los componentes de infraestructura se realizará al final de cada mes según los consumos realizados por cada uno de estos componentes especificado en la tabla de la sección 11.8. Especificaciones de capacidades de los servicios de seguridad. (considerar dev, qa, prd) y compartidos.

En situaciones donde el servicio se inicie en un día que no coincida con el comienzo de un mes calendario, se aplicara el prorrateo. El prorrateo consistirá en calcular la proporción del servicio utilizado desde la fecha de inicio hasta el final del mes en curso y facturar únicamente por ese período inicial de manera proporcional.

El Contratista emitirá un informe a cada fin de mes indicando los consumos realizados por cada uno de los componentes, reportes de monitoreo, Incidencias generadas, así como las soluciones realizadas, además de recomendaciones de mejora de ser el caso.

El Banco revisará el informe como máximo en 5 días calendario y si hubiera

alguna observación se le indicará al Contratista a través de correo electrónico al líder de proyecto del Contratista para la subsanación respectiva, para lo cual el Contratista tendrá 5 días calendarios adicionales como máximo para la subsanación. Una vez concluida la revisión por parte del Banco se emitirá un informe técnico y posteriormente el acta de conformidad para el pago.

El responsable de la aprobación del informe técnico será el área siguiente:

- Oficina de Seguridad Informática

El responsable del acta de conformidad será la Subgerencia de Innovación Digital de la Gerencia Banca Digital.

Los documentos a entregar por parte del Contratista para el pago serán:

- Carta simple dirigida al subgerente de compras de la gerencia de administración y logística
- Acta de conformidad suscrita por la Subgerencia de Innovación Digital de la Gerencia Banca Digital.
- Comprobante de pago.
- Informe técnico por parte de la Gerencia de TI especificado anteriormente.
- Copia del contrato.

b.4 Para el Pago del Soporte Técnico

b.4.1 Pago Mensual de Soporte Técnico

El pago por el soporte y mantenimiento de la infraestructura y seguridad se realizará al final de cada mes, hasta el final del contrato, iniciándose este soporte y mantenimiento al finalizar la implementación del ambiente de producción como indicará el informe técnico de aprobación del ambiente de producción (PRD).

En situaciones donde el servicio se inicie en un día que no coincida con el comienzo de un mes calendario, se aplicara el prorrateo. El prorrateo consistirá en calcular la proporción del servicio utilizado desde la fecha de inicio hasta el final del mes en curso y facturar únicamente por ese período inicial de manera proporcional.

El Contratista emitirá un informe a cada fin de mes indicando los incidentes y atenciones realizadas, así como las soluciones implementadas, además de recomendaciones de mejora de ser el caso.

El Banco revisará el informe como máximo en 5 días calendario y si hubiera alguna observación se le indicará al Contratista a través de correo electrónico al líder de proyecto del Contratista para la subsanación respectiva, para lo cual el Contratista tendrá 5 días calendarios adicionales como máximo para la subsanación. Una vez concluida la revisión por parte del Banco se emitirá un informe técnico y posteriormente el acta de conformidad para el pago.

Los responsables de la aprobación del informe técnico serán las áreas siguientes es:

- Subgerencia de Construcción
- Subgerencia de Producción
- Oficina de Seguridad Informática

El responsable del acta de conformidad será la Subgerencia de Innovación Digital de la Gerencia Banca Digital.

Los documentos a entregar por parte del Contratista para el pago serán:

- Carta simple dirigida al subgerente de compras de la gerencia de administración y logística

- Acta de conformidad suscrita por la Subgerencia de Innovación Digital de la Gerencia Banca Digital.
- Comprobante de pago.
- Informe técnico por parte de la Gerencia de TI especificado anteriormente.
- Copia del contrato.

La Entidad debe pagar las contraprestaciones pactadas a favor del Contratista dentro de los 15 días calendario siguiente a la conformidad de los servicios, siempre que se verifiquen las condiciones establecidas en el contrato.
Los informes remitidos en esta sección por parte del contratista serán coordinados para determinar el contenido de los mismos y el formato de estos debiendo estar definidos en el plan de trabajo.

Componente Opcional

Cuenta DNI

El pago se efectuará contra el Acta de Conformidad del diseño, desarrollo e implementación del componente opcional Cuenta DNI. Este pago se realizará conforme al sistema de precio unitario. El precio unitario será determinado por la propuesta comercial presentada por el Contratista.

Servicio de Mejora Continua

El pago se llevará a cabo mensualmente, o según lo acordado con el Banco, una vez se haya recibido y aprobado el Acta de Conformidad correspondiente. Este pago se realizará conforme al sistema de precio unitario y basado en el consumo de horas utilizadas durante el periodo facturado. Los precios unitarios serán determinados por la propuesta comercial presentada por el Contratista.

1.3.5 MEDIDAS DE CONTROL DURANTE LA EJECUCION CONTRACTUAL Y CONFORMIDAD DEL SERVICIO

Administrador de Contrato
La Subgerencia de Innovación Digital de la Gerencia de Banca Digital, se encargará de la administración del contrato durante la ejecución del proyecto, siendo responsable de la supervisión y coordinación de la prestación contratada.

Área Responsable del Control de la Implementación
La Subgerencia de Producción, Subgerencia de Construcción de Aplicaciones y la Oficina de Seguridad de la Gerencia Tecnologías de Información serán responsables de la supervisión y coordinación del servicio de la implementación nueva plataforma bancaria para los canales digitales Banca Móvil y Banca por Internet.

1.3.6 DEL CODIGO DE ETICA DEL BANCO DE LA NACION

El proveedor del servicio declara bajo juramento conocer que el Banco cuenta con un código de Ética, cuyo objetivo está orientado a establecer valores instituciones, principios, derechos, deberes y prohibiciones éticas. Por lo tanto, el proveedor del servicio se compromete a tomar conocimiento del contenido de este, a través del enlace: www.bn.com.pe/nosotros/archivos/CodigoEticaBN.pdf.

1.3.7 ANTICORRUPCION

El Proveedor declara y garantiza no haber, directa o indirectamente, o tratándose de una persona jurídica a través de sus socios, integrantes de los órganos de administración, apoderados,

representantes legales, funcionarios, asesores o personas vinculadas a las que se refiere el artículo 7 del Reglamento de la Ley de Contrataciones del Estado, ofrecido, negociado o efectuado, cualquier pago o, en general, cualquier beneficio o incentivo ilegal en relación con el contrato/orden de servicio.

Asimismo, el Proveedor se obliga a conducirse en todo momento, durante la ejecución del contrato, con honestidad, probidad, veracidad e integridad y de no cometer actos ilegales o de corrupción, directa o indirectamente o a través de sus socios, accionistas, participacioncitas, integrantes de los órganos de administración, apoderados, representantes legales, funcionarios, asesores y personas vinculadas a las que se refiere el artículo 7 del Reglamento de la Ley de Contrataciones del Estado.

Además, el Proveedor se compromete a i) comunicar a las autoridades competentes, de manera directa y oportuna, cualquier acto o conducta ilícita o corrupta de la que tuviera conocimiento; y ii) adoptar medidas técnicas, organizativas y/o de personal apropiadas para evitar los referidos actos o prácticas.

1.3.8 RESPONSABILIDAD DEL PROVEEDOR POR VICIOS OCULTOS

El Proveedor es responsable por la calidad ofrecida y por los vicios ocultos de los servicios ofertados por un plazo de dos (02) años contados a partir de las conformidades otorgadas por cada entregable por el Banco de la Nación.

1.3.9 GARANTÍA FINANCIERA

El postor adjudicado con la buena pro del concurso de méritos entregará para el perfeccionamiento del contrato la garantía financiera (carta fianza) de fiel cumplimiento de contrato.

La garantía que se presente debe ser incondicionales, solidarias, irrevocables y de realización automática en el país, al solo requerimiento del Banco de la Nación. Asimismo, debe ser emitida por empresas que se encuentren bajo la supervisión directa de la Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones y que cuenten con clasificación de riesgo B o superior. Asimismo, deben estar autorizadas para emitir garantías; o estar consideradas en la última lista de Bancos extranjeros de primera categoría que periódicamente publica el Banco Central de Reserva del Perú.

La garantía financiera (cartas fianza) deberá ser emitida a favor del Banco de la Nación, por los conceptos, montos y vigencias siguientes:

- Garantía de fiel cumplimiento del contrato: por una suma equivalente al diez por ciento (10%) del monto del contrato original, la misma que debe mantenerse vigente hasta la conformidad de la recepción de la prestación.

1.3.12 CONFIDENCIALIDAD

Toda la información entregada por el Banco de la Nación al postor del servicio tiene carácter confidencial.

Cualquier copia, publicación, divulgación, distribución, total o parcial, interceptación sin autorización expresa por parte del Banco de la Nación o con fines no autorizados por el Banco de la Nación, de los documentos o información que describan la arquitectura y operación de las aplicaciones y base de datos del Banco de la Nación, serán motivo para la inmediata rescisión del vínculo contractual y del inicio de acciones legales que el Banco de la Nación considere. Su incumplimiento de la confidencialidad acarrea un incumplimiento a las obligaciones contractuales del presente termino de referencia.

1.4 EL COMITÉ DE CONCURSO DE MERITOS

El presente Concurso de Méritos, se desarrollará de acuerdo con lo establecido en las presentes Bases, y será conducido por el Comité de Concurso de Méritos designado, quienes actúan en forma colegiada cuentan con autonomía para interpretar y adoptar las decisiones que sean pertinentes, las cuales no requieren ratificación de algún funcionario del Banco de la Nación.

Ante la ausencia de un miembro titular en el Comité, este será reemplazado por el suplente designado, siempre y cuando se respete la conformación aprobada por la Gerencia de Administración y Logística del Banco de la Nación. El suplente solo reemplazará al titular en las sesiones del Comité en las que este último se encuentre ausente.

En caso de ausencia de un titular y su suplente, la Gerencia que los designó, deberá designar con carácter de urgente a un miembro adicional, en reemplazo de ambos por las sesiones que cualquiera de ellos no pueda asistir.

Para sesionar y adoptar acuerdos válidos, el Comité del Concurso de Méritos deberán tener un quórum igual a la totalidad de sus miembros titulares o suplentes y los acuerdos serán adoptados por mayoría y consignados en Actas.

CAPÍTULO II

BASE NORMATIVA

- Ley N° 29733 – Ley de protección de datos personales
- Decreto Legislativo N° 1412-2018 - Decreto Legislativo que aprueba la Ley de Gobierno Digital.
- Decreto Supremo N.º 050-2018-PCM - Decreto que establece la definición de Seguridad Digital de ámbito nacional, en el cumplimiento con la Segunda Disposición Complementaria Final de la Ley N°30618, Ley que modifica el Decreto Legislativo N°1441.
- Decreto Supremo N.º 029-2021-PCM - Decreto Supremo que aprueba el Reglamento de la Ley de Gobierno Digital
- Decreto Supremo N° 085-2023-PCM - Decreto Supremo que aprueba la Política Nacional de Transformación Digital al 2030
- Resolución SBS N° 504-2021 – Aprueba el reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad.
- Resolución SBS N° 6523-2013 y sus modificatorias – Reglamento de Tarjetas de Crédito y Débito.
- Directiva BN-CIR-2100-216-05 Gestión de riesgos de nuevos productos o cambios importantes en el ambiente de negocios, operativo o informático del Banco
- Directiva BN-MAN-2100-010-06 Manual para el tratamiento de las contrataciones / subcontrataciones significativas en el Banco de la Nación
- Directiva BN-DIR-7700-272-03 Gestión del Portafolio y Proyectos.
- Directiva BN-DIR-8300-147-01 Ciclo de Vida del Software
- Directiva BN-DIR-5500-152-01 Contratación de Servicios Financieros en el BN
- Directiva BN-DIR-2400-112 Gestión de claves criptográficas
- Las demás disposiciones que resulten aplicables.

CAPÍTULO III

PROCESO DE CONCURSO DE MERITOS

3.1 ETAPAS DEL CONCURSO DE MERITOS

El Concurso de Méritos se desarrolla conforme a las disposiciones del Cronograma establecido en las presentes Bases que se detalla:

Cronograma del Concurso de Méritos

N°	Etapa	Periodo
1	Convocatoria	29/08/2024
2	Formulación de Consultas	Del 02/09/2024 al 09/09/2024
3	Absolución de Consultas	13/09/2024
4	Integración de Bases	16/09/2024
5	Presentación de Propuestas (Acto Público) A las 09:00 horas en el piso 8 de la Sede Central del BN (Av. Javier Prado Este N° 2499 - San Borja)	23/09/2024
6	Evaluación de Propuestas	Del 24/09/2024 al 25/09/2024
7	Otorgamiento de la Buena Pro	26/09/2024
8	Comunicación de Resultados	26/09/2024

Las etapas del Concurso de Méritos son las siguientes:

3.2.1 Convocatoria

Se efectuará a través de invitaciones a través de correo electrónico, a las empresas que ofrecen el servicio requerido, adjuntando archivo con las Bases aprobadas.

3.2.2 Formulación de Consultas

Las consultas que formulen los participantes deben estar referidas al alcance o contenido de cualquier aspecto de las Bases, deberán ser enviadas a los correos electrónicos: cquevedo@bn.com.pe, avalenzuela@bn.com.pe y rortiz@bn.com.pe, respetando el plazo de presentación establecido en el Cronograma, las consultas que presenten fuera del plazo establecido o enviadas por algún otro medio, se considerarán como no presentadas y no serán tomados en cuenta por el Comité que conduce el proceso de concurso de méritos.

3.2.3 Absolución de Consultas

El Comité del Concurso de Méritos absolverá las consultas presentadas por los participantes, la Absolución de Consultas será comunicada a todos los participantes a través de los correos electrónicos que hayan designado, dentro de los plazos establecidos en el Cronograma del proceso de concurso de méritos.

3.2.4 Integración de Bases

Las Bases Integradas constituyen las reglas definitivas del Concurso de

Méritos, las que contendrán las correcciones, precisiones y/o modificaciones producidas como consecuencia de la Absolución de las Consultas.

3.2.5 Presentación de Propuestas

La presentación de propuestas se realizará en acto público, en el lugar, fecha y hora señaladas en el cronograma del Concurso de Méritos, con la participación de Notario Público.

El acto se inicia cuando el Comité empieza a llamar a los participantes para que entreguen sus propuestas. Si al momento de ser llamado el participante no se encuentra presente, se le tendrá por desistido.

Las propuestas se presentarán en dos (2) sobres cerrados, que contendrán la propuesta técnica y económica respectivamente, la que debe estar foliada correlativamente empezando por el número uno y deben llevar el sello y la rúbrica del postor o de su representante legal o mandatario designado para dicho fin.

Después de recibidas las propuestas, el Comité procederá a abrir los sobres que contienen la propuesta técnica y económica de cada postor, a fin de verificar que se encuentren los documentos presentados por cada postor sean los solicitados en las Bases.

Todos los documentos que contengan información referida a los requisitos para la admisión de propuestas, factores de evaluación y requisitos de calificación se presentarán en idioma castellano o, en su defecto, acompañados de la respectiva traducción por traductor público juramentado o traductor colegiado certificado, salvo el caso de la información técnica complementaria contenida en folletos, instructivos, catálogos o similares, que podrá ser presentada en el idioma original. El postor será responsable de la exactitud y veracidad de dichos documentos.

En el caso que de la revisión de la propuesta se adviertan defectos de forma, tales como errores u omisiones subsanables en los documentos presentados que no modifiquen el alcance de la propuesta técnica y económica, se puede otorgar plazo para subsanar la propuesta técnica.

Después de abierto cada sobre que contiene la propuesta técnica y económica verificado que contengan los requeridos como documentación de presentación obligatoria, el Notario procederá a sellar y firmar cada hoja de los documentos de la propuesta técnica y económica.

Al terminar el acto público, se levantará un acta, la cual será suscrita por el Notario, por todos sus miembros.

- ✓ **Sobre: Propuesta Técnica**
  Se presentará en un original con el siguiente rotulado:

Señores Banco de la Nación Av. Javier Prado Este N° 2499 - San Borja **Att.: Comité del Concurso de Méritos** **CONCURSO DE MERITOS N° 0004-2024-BN** Servicio de implementación de nueva plataforma bancaria para canales digitales banca móvil y banca por internet del Banco de la Nación SOBRE : PROPUESTA TÉCNICA [NOMBRE / RAZÓN SOCIAL DEL POSTOR]

El Sobre de la propuesta técnica contendrá, además de un índice de documentos, la siguiente documentación:

Documentación de Presentación Obligatoria:

a) Declaración Jurada de Datos del Postor. (**Formato Nº 1**).

b) Documento que acredite la representación de quien suscribe la oferta.

   Copia del Certificado de Vigencia de Poder del representante legal, apoderado o mandatario designado para tal efecto.

   En el caso de consorcios, este documento debe ser presentado por cada uno de los integrantes del consorcio que suscriba la promesa de consorcio, según corresponda.

c) Declaración Jurada de cumplir con los requisitos para ser postor en el presente proceso de concurso de méritos. **(Formato Nº 2).**

d) Declaración Jurada de Cumplimiento de los Términos de Referencia contenidos en el Anexo N° 1 de la presente Bases. **(Formato Nº 3).**

e) Declaración Jurada de Plazo de Prestación del Servicio. **(Formato Nº 4).**

f) Promesa de Consorcio con firmas legalizadas, de ser el caso, en la que se consigne los integrantes, el representante común, el domicilio común y las obligaciones a las que se compromete cada uno de los integrantes del consorcio, así como el porcentaje equivalente a dichas obligaciones. (**Formato Nº 5**).

g) Detalle de la Experiencia del Postor en la Especialidad **(Formato N° 7)**.

h) De ser el caso, Declaración Jurada de Reorganización Societaria (**Formato N° 8**).

i) Documentos para Acreditar los Requisitos de Calificación.
   Presentación de documentos que acreditarán el cumplimiento de los

"Requisitos de Calificación" que se detallan en los términos de referencia.

Referido a Implementación de la Arquitectura en la Nube

j) El proveedor de nube debe ser un proveedor de servicios de nube pública y por lo tanto debe formar parte del cuadrante de Líderes en el Cuadrante Mágico de Gartner vigente para servicios de infraestructura y plataforma en la nube.

k) El participante en su oferta presentará en copia simple las siguientes certificaciones de la empresa que brindará el servicio de nube :[1]

- PCI-DSS: Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago.
- Cloud Security Alliance (CSA): controles de la alianza de seguridad en la nube.
- ISO 9001: estándar de calidad internacional
- ISO 22301: implementación, mantenimiento y mejora a sistemas de continuidad de negocio.
- ISO 27001: controles de administración de seguridad
- ISO 27017: controles específicos de nube
- ISO 27018: protección de datos personales o[2] ISO 27701: sistema de gestión sobre la privacidad y gestión del contenido
- SOC 1: informe de controles de auditoría
- SOC 2: informe de seguridad, disponibilidad y confidencialidad
- SOC 3: informe de controles generales

El Comité de Selección responsable de la conducción de Concurso de Méritos N° 0004-2024-BN, verificará la presentación de los documentos requeridos con carácter de presentación obligatoria. De no cumplir con lo requerido, la oferta se considera no admitida.

✓ **Sobre: Propuesta Económica**

Se presentará en un original con el siguiente rotulado:

Señores Banco de la Nación Av. Javier Prado Este N° 2499 - San Borja **Att.: Comité del Concurso de Méritos** **CONCURSO DE MERITOS N° 0004-2024-BN** Servicio de implementación de nueva plataforma bancaria para canales digitales banca móvil y banca por internet del Banco de la Nación SOBRE : PROPUESTA ECONOMICA [NOMBRE / RAZÓN SOCIAL DEL POSTOR]

[1] Pliego de Consultas N° 01-2024 - Concurso de Méritos (Consulta N° 1 PERÚ APP, Consulta N° 6 PERÚ APP y Consulta N° 43 TCO LATAM).
[2] Pliego de Consultas N° 01-2024 - Concurso de Méritos (Consulta N° 1 PERÚ APP, Consulta N° 6 PERÚ APP y Consulta N° 43 TCO LATAM).

La Propuesta Económica, deberá incluir obligatoriamente su oferta en Soles (S/), y el detalle de precios unitarios conforme a los establecido en las Bases (**Formato Nº 6**) incluidos todos los tributos, los costos laborales conforme a la legislación vigente; así como, cualquier otro concepto que pueda tener incidencia sobre el costo del servicio a contratar.

El monto total de la propuesta económica y los subtotales que lo componen deberán ser expresados con dos decimales. Los precios unitarios podrán ser expresados con más de dos decimales.

En el documento que contiene el precio ofertado u oferta económica puede subsanarse la rúbrica y la foliación.

En caso de divergencia entre el precio cotizado en números y letras, prevalece este último. Cuando se advierta errores aritméticos, corresponde su corrección al Comité, debiendo constar dicha rectificación en el acta respectiva; en este último caso, dicha corrección no implica la variación de los precios unitarios ofertados.

3.2.6 Evaluación de Propuestas

La evaluación de propuestas se realizará en dos (2) etapas: La evaluación económica y la evaluación técnica.

La información contenida en la oferta debe ser objetiva, clara, precisa y congruente entre sí y debe encontrarse conforme con lo requerido en las bases, a fin de que el Comité del Concurso de Méritos encargado de la Contratación, puedan apreciar el real alcance de la misma y su idoneidad para satisfacer el requerimiento de la Entidad, lo contrario, por los riesgos que implica, determinará que la Oferta sea desestimada.

No es función del Comité del Concurso de Méritos, interpretar el alcance de una oferta, esclarecer ambigüedades, o precisar contradicciones o imprecisiones, sino evaluar las ofertas en virtud a las bases, realizando un análisis integral que permita generar convicción de lo realmente ofertado, sin posibilidad de inferir o interpretar hecho alguno.

3.2.6.1 Evaluación Económica

Para determinar la oferta con el mejor puntaje y el orden de prelación de las ofertas, se aplicará el siguiente procedimiento:

1. **Puntaje Total:** 100 puntos

2. **Evaluación del Precio**
   Para determinar la oferta con el mejor puntaje, consistirá en asignar el puntaje máximo establecido a la propuesta económica de menor monto. Al resto de propuestas se les asignará un puntaje inversamente proporcional, según la siguiente fórmula:

$$Pi = \frac{Om \times PMP}{Oi}$$

Donde:

I	=	Propuesta
Pi	=	Puntaje de la propuesta económica i
Oi	=	Propuesta Económica i
Om	=	Propuesta Económica de monto o precio más bajo
PMPE	=	Puntaje Máximo de la Propuesta Económica

3.2.6.2 Evaluación Técnica

Se verificarán las ofertas técnicas de los postores que en la evaluación económica han obtenido el primer y segundo puesto en el orden de prelación, en caso alguna no cumpla con los requisitos de calificación se continuará con la evaluación técnica siguiendo el orden de prelación.

La evaluación técnica consistirá en la verificación de los requisitos de calificación. Se verificará que la propuesta técnica cumpla con los requerimientos técnicos mínimos contenidos en las presentes Bases. Las propuestas que no cumplan dichos requerimientos quedarán como descalificadas.

En aquellos casos en los que se hubiese otorgado plazo para la subsanación de la propuesta, el Comité de Selección deberá determinar si se cumplió o no con la subsanación solicitada. Si luego de vencido el plazo otorgado, no se cumple con la subsanación, el Comité tendrá la propuesta por no admitida.

Una vez cumplida la subsanación de la propuesta o vencido el plazo otorgado para dicho efecto, se continuará con la evaluación de las propuestas técnicas admitidas, verificando que cumplan con los requisitos de calificación. La oferta que no cumpla con los requisitos de calificación es descalificada.

3.2.7 Otorgamiento de la Buena Pro

Una vez evaluadas las propuestas el Comité de Selección procederá a otorgar la Buena Pro a la propuesta ganadora, de acuerdo con el cuadro comparativo en el que se consignará el orden de prelación en que han quedado calificados.

En el supuesto que dos (2) o más ofertas empaten, la determinación del orden de prelación de las ofertas empatadas se realiza a través de sorteo efectuado por un Notario Público.

En los casos de haberse presentado una sola oferta a los Concursos de Méritos, el Comité, a su sola decisión, podrá otorgar la Buena Pro al único postor, siempre que cumpla con los requisitos de las Bases.

3.2.8 Comunicación de Resultados

El presidente del Comité comunicará los resultados del Concurso de Méritos, mediante correo electrónico dirigido a todos los postores.

3.3 Procedimiento para la Atención de Solicitudes o Reclamos Presentados por Postores

En el supuesto que algún postor presente una solicitud, o presente un reclamo, respecto a cualquier acto que haya realizado el Comité del Concurso de Méritos en el ejercicio de sus funciones, se deberá seguir el procedimiento que se detalla a continuación (no se incluyen en este procedimiento, las consultas y/o observaciones que se efectúen dentro del Concurso de Méritos, cuando correspondan estos a la etapa del Concurso):

a) El Postor deberá presentar su reclamo o solicitud, en el plazo máximo de tres (3) días hábiles, contados a partir del día siguiente de la comunicación de los resultados del proceso efectuado por el Banco, en la Sección Trámite Documentario sito en la Calle Arqueología N° 120 - San Borja en el horario de 08:30 a 16:30 Horas, quien deberá remitirlo a la Gerencia de Administración y Logística. Dicha Gerencia, de manera inmediata, enviará el documento a los miembros del Comité de Concurso de Méritos para su revisión, quienes emitirán de manera colegiada, el informe técnico respectivo, dando respuesta a cada una de las solicitudes, reclamos y/o pedidos formulados por el postor. El citado documento también es remitido a la Subgerencia Compras para el seguimiento respectivo. Dicho informe sirve como sustento para brindar respuesta a la solicitud o reclamo presentado por el postor.

b) El informe deberá ser emitido dentro de los tres (3) días hábiles siguientes desde la fecha de recepción del documento, por parte del comité, bajo responsabilidad. En caso se requiere de mayor tiempo para emitir el informe, por complejidad del asunto a contestar o por necesitar información y/o documentación de otras áreas del Banco, se puede ampliar el plazo por 3 días hábiles adicionales por una sola vez.

c) Dicho informe será remitido a la Subgerencia Compras de la Gerencia de Administración y Logística juntamente con el Expediente de Contratación para su revisión, análisis, opinión y elaboración del proyecto de carta de respuesta, previa consulta con la Gerencia Legal, de corresponder. (en caso exista un aspecto jurídico para su evaluación).

d) La Gerencia de Administración y Logística, en un plazo máximo de tres (3) días hábiles, formalizará la carta de respuesta y solamente en caso existan aspectos de carácter jurídico en la respuesta a brindar, procederá la visación de la Gerencia Legal.

3.5 Del Perfeccionamiento del Contrato

Dentro del plazo de ocho (8) días hábiles siguientes al otorgamiento de la Buena Pro, el postor ganador de la buena pro debe presentar los siguientes documentos para perfeccionar el contrato:

a) Garantía de fiel cumplimiento del contrato.
b) Contrato de consorcio con firmas legalizadas ante Notario de cada uno de los integrantes, de ser el caso.

c) Código de cuenta interbancaria (CCI) o, en el caso de proveedores no domiciliados, el número de su cuenta bancaria y la entidad bancaria en el exterior.
d) Copia de la vigencia del poder del representante legal de la empresa que acredite que cuenta con facultades para perfeccionar el contrato, cuando corresponda.
e) Copia de DNI del representante legal.
f) Domicilio para efectos de la notificación durante la ejecución del contrato.
g) Autorización de notificaciones por el Banco de la Nación, durante la ejecución contractual mediante medios electrónicos de comunicación (**Formato N° 9**).
h) El postor ganador deberá presentar la documentación que acredite: La Formación Académica, capacitación y experiencia exigida para el personal no clave requeridos en el numerales 26.3 Personal de Desarrollo y Soporte Técnico y 26.2 Recursos de personal para la Mejora Continua del Servicio.
i) Carta u otro documento oficial que acredite la condición de "partner" con una empresa que brinda servicios en la nube, concordante con el numeral 9. Arquitectura Tecnológica Requerida de los TDR.

j) Seguridad y Salud en el Trabajo
El ganador de la Buena PRO a la suscripción del contrato deberá presentar obligatoriamente una Declaración Jurada que cumple las disposiciones establecidas en la Ley N° 29783 - Ley de Seguridad y Salud en el Trabajo y su Reglamento.

k) Prevención del Lavado de Activos y del Financiamiento del Terrorismo
A la suscripción del contrato, el ganador de la buena pro deberá presentar la siguiente Información:
- Nombres y Apellidos completos o denominación o razón social, el caso se trate de una persona jurídica.
- Registro Único de Contribuyentes (RUC), o registro equivalente para no domiciliados, de ser el caso.
- Tipo u número de documento de Identidad, en caso de trate de una persona natural.
- Dirección de la oficina o local principal.
- Años de Experiencia en el mercado.
- Rubros en los que el proveedor brinda sus productos o servicios.
- Identificación de los accionistas, socios o asociados que tengan directa o indirectamente el 25 % del capital social, aporte o participación de la persona jurídica y del nombre del representante legal, considerando la información requerida para las personas naturales.
- Declaración Jurada de no contar con antecedentes penales del proveedor, de ser el caso.
- No encontrarse incluido en la lista emitida por la Oficina de Control de Activos Extranjeros del Departamento de Tesoro de los Estados Unidos de América (OFAC).

De acuerdo con el Anexo N° 1 de la Resolución S.B.S. N° 2660-2015 Reglamento de Gestión de Riesgos de Lavado de Activos y del Financiamiento del Terrorismo, el proveedor adjudicado con la buena pro deberá cumplir con lo especificado por dicha Resolución, lo cual será verificado por el Banco antes de la firma del contrato.
Para tal efecto, deberá presentar el **(Formato N° 10)** debidamente completado.

l) Declaración Jurada de no encontrarse inscrito en el Registro de Deudores de Reparaciones Civiles (REDERECI). **(Formato N° 11)**
m) Declaración Jurada de no estar Inhabilitado para contratar con el Estado. **(Formato N° 12)**

En un plazo que no podrá exceder de los dos (02) días hábiles siguientes de presentados los documentos, de existir observaciones el BN solicitará la subsanación de los requisitos, en un plazo adicional de cuatro (04) días contados

desde el día siguiente de la notificación al postor. De no existir observaciones, el BN solicitará al postor que en un plazo no mayor de (02) días hábiles comunique sobre sus observaciones al Proyecto de Contrato contenido en las Bases, luego de lo cual, las partes tendrán un plazo de cuatro (04) días hábiles para realizar los ajustes que resulten necesarios dentro de los alcances del servicio contratado y suscribir el contrato. Dicho plazo podrá ser ampliado por acuerdo de las partes.

Cuando no se perfeccione el contrato, por causa imputable al postor, éste pierde automáticamente la buena pro; en tal supuesto, la Subgerencia de Compras como órgano encargado de las contrataciones (OEC) del BN, en un plazo máximo de tres (3) días hábiles, requiere al postor que ocupó el segundo lugar que presente los documentos para perfeccionar el contrato en los mismos plazos previstos en el párrafo anterior. Si el postor no perfecciona el contrato, el órgano encargado de las contrataciones del BN declara desierto el proceso de concurso de méritos.

3.5 DISPOSICIONES FINALES

a) Los servicios financieros que contrata el Banco, no se enmarcan dentro de los procedimientos administrativos regulados por el TUO de la Ley del Procedimiento Administrativo General, aprobado por Decreto Supremo N° 004-2019-JUS, por lo que no constituye el Concurso de Méritos llevado a cabo bajo los alcances de la Directiva BN-DIR-5500-152-01, un procedimiento o acto administrativo que pueda ser sujeto de recurso impugnatorio alguno.

b) El Comité del Concurso de Méritos culminará sus funciones con la entrega del informe correspondiente a la Gerencia de Administración y Logística, lo que se producirá luego de la notificación en acto público del otorgamiento de la buena pro del Concurso de Méritos.

Anexos

Anexo N° 1

IMPLEMENTACIÓN DE LA NUEVA PLATAFORMA BANCARIA PARA LOS CANALES DIGITALES BANCA MÓVIL Y BANCA POR INTERNET DEL BANCO DE LA NACIÓN

TÉRMINOS DE REFERENCIA
Versión 4.0

1. DENOMINACIÓN DEL SERVICIO

Implementación de la nueva plataforma bancaria para los canales digitales Banca Móvil y Banca por Internet del Banco de la Nación.

2. FINALIDAD PÚBLICA

Ofrecer a todos los ciudadanos el acceso a servicios bancarios de calidad, fomentando el uso de los canales digitales promoviendo una mayor adopción de tecnologías financieras.

3. ANTECEDENTES

- El Banco de la Nación es una empresa con potestades públicas, integrante del Sector Economía y Finanzas, que opera con autonomía económica, financiera y administrativa, el cual se rige por su Estatuto, por el Decreto Legislativo N° 1031, Decreto Legislativo que promueve la eficiencia de la actividad empresarial del Estado y su Reglamento, y el artículo 33° de la Ley N.º 26702, Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros, y supletoriamente por los demás artículos de dicha Ley General o sus modificatorias.
- De acuerdo a lo señalado en el artículo 3° del Estatuto, el Banco se rige por este, por el Decreto Legislativo N° 1031, Decreto Legislativo que promueve la eficiencia de la actividad empresarial del Estado y su Reglamento, y el artículo 33° de la Ley Nº 26702, Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros, y supletoriamente por los demás artículos de dicha Ley General o sus modificatorias.
- El artículo 4° del Estatuto establece, entre otros, que el BN tiene como objeto realizar operaciones y servicios para la inclusión financiera y con la finalidad de contribuir al desarrollo económico e inclusión social, con sujeción a lo señalado en la Política Nacional de Inclusión Financiera (PNIF).
- Con fecha 26/02/2014, se actualiza la normatividad vigente relacionada a las operaciones que se realizan en la AGENCIA VIRTUAL a través del Canal de Atención BANCA POR INTERNET del sistema Internet del Banco mediante la Circular N° BN-CIR-7900-058-05.
- Con fecha 11/04/2016, se aprueba la modificación de las nuevas transacciones de transferencias interbancarias en línea y pago de Tarjetas de Crédito de otros Bancos en línea por medio de Canal Banca por Internet mediante la Circular BN-ClR-3100-058-05 BANCA POR INTERNET.

- Con fecha 09/07/2014, se aprobó la circular Banca por Internet BN-CIR-3100-058-05 Rev.0 en cual actualiza el procedimiento de afiliación y generación de la clave de internet a través del Portal Web del Banco.
- Con fecha 23/11/2016, se adecua el acuerdo a las nuevas transacciones en línea por medio de Canal Banca por Internet.
- Con fecha 26/11/2020, se establecen normas y procedimientos relacionados a la afiliación, activación y vinculación, desafiliación y uso de la CLAVE DINÁMICA DIGITAL, mecanismo de autenticación, alternativo al token físico, que permite a los Clientes autorizar sus transacciones en los canales Banca por Internet – Banca por Internet y App BN - Banca Móvil, mediante la circular N° BN-CIR - 7900-414-01.
- Con fecha 17/06/2020, se aprueba la creación de la Gerencia de Banca Digital mediante el Acuerdo de Directorio N° 2315.
- Con fecha 27/09/2023, se actualiza el procedimiento que describen las actividades realizadas para efectuar la conciliación diaria y contabilización del canal app Banca Móvil.

4. GLOSARIO DE TÉRMINOS

- **Actividades de Contención**

Actividades inmediatas para evitar que el incidente siga produciendo daños.

- **Almacenamiento Estructurado**

Información que se suele encontrar en la mayoría de las bases de datos. Son archivos de tipo texto que se suelen mostrar en filas y columnas con títulos. Son datos que pueden ser ordenados y procesados fácilmente por todas las herramientas de minería de datos.

- **Almacenamiento No Estructurado**

Los datos no estructurados, generalmente son datos binarios que no tienen estructura interna identificable. Es un conglomerado masivo y desorganizado de varios objetos que no tienen valor hasta que se identifican y almacenan de manera organizada.

- **Ataque DDoS**

Tipo de ataque a un sistema de cómputo o de comunicaciones que intenta agotar los recursos del sistema (como el ancho de banda de los enlaces de Internet del prestador del servicio, capacidad de procesamiento de los equipos de cómputo o comunicaciones), lanzando infinidad de peticiones aparentemente válidas desde uno o diversos orígenes, con la finalidad de saturar el servicio haciéndolo indisponible a los usuarios legítimos (denegación del servicio).

- **API:**

Una API, o interfaz de programación de aplicaciones, es un conjunto de definiciones y protocolos que permiten a dos componentes de software comunicarse entre sí. En otras palabras, es una forma de que dos aplicaciones se entiendan y se

comuniquen.

- **API Gateway:**

Una API Gateway es un servicio que actúa como intermediario entre las aplicaciones clientes y los servicios de Back-End. Su función principal es proporcionar un único punto de acceso a las API de los servicios de Back-End, lo que simplifica el desarrollo y la gestión de las aplicaciones clientes.

- **Banca Móvil**

Esta aplicación facilita la realización de consultas y transacciones financieras con cargo en cuenta de ahorros, créditos y otros, mediante teléfonos móviles inteligentes (Smartphone).

- **Banca por Internet**

Esta aplicación facilita la realización de consultas y transacciones financieras con cargo en cuenta de ahorros, créditos y otros, mediante una página web.

- **BDUC**

Base de Datos Única de Clientes

- **Bitácora, Registro o LOG**

Es un archivo o una base de datos que almacena información sobre eventos o acciones que afectan a un proceso, aplicación o sistema.

- **BYOL**

BYOL o "bring your own license" es el proceso de incorporar licencias locales, compradas previamente. Cuando usa sus propias licencias, el costo de licencia del producto que incorpora ya no se incluye en el precio de la instancia. Cuando incorpora licencias, es responsable de administrarlas.

- **Canales Digitales**

Los canales digitales del Banco de la Nación son plataformas y servicios electrónicos que permiten a los clientes realizar operaciones financieras y acceder a servicios bancarios a través de medios digitales. Estos canales facilitan la interacción remota con el Banco, brindando comodidad y acceso conveniente a diversas transacciones. Algunos de los canales digitales comunes incluyen: Banca por Internet y Banca Móvil.

- **Computación en la Nube**

La computación en la nube es un modelo para permitir el acceso bajo demanda, conveniente y ubicuo a un grupo compartido de recursos informáticos configurables (p. Ej., redes, servidores, almacenamiento, aplicaciones y servicios) que se pueden aprovisionar y liberar rápidamente con un esfuerzo mínimo de administración.

El término Cloud o Nube, es una alusión metafórica a Internet. Mediante este sistema

los clientes pueden acceder a determinados servicios que se encuentran almacenados de forma permanente en servidores remotos y cuando un cliente así lo solicita, se hace inmediatamente disponible en sus equipos de escritorio, lugares de trabajo, dispositivos portátiles, etc. Según las necesidades requeridas de cada momento de forma que la computación en la nube se ha constituido como un auténtico "modelo a la carta" para la prestación de servicios relacionados con el software, las aplicaciones y las infraestructuras tecnológicas.

- **Core/Núcleo**

Unidad independiente real de procesamiento central, perteneciente a un procesador.

- **CCI (Código de Cuenta Interbancario)**

Código que identifica una cuenta en todo el sistema bancario. Cada cuenta tiene asignado un CCI que la identifica en forma única y segura para realizar transferencias interbancarias.

- **Clave de Internet**

Es la clave que permite a los clientes acceder a los canales virtuales del Banco, en modo de consulta y Es generada de manera personal por el titular de una cuenta de ahorros en el proceso de enrolamiento a los canales digitales. Esta clave se convierte en un código secreto y confidencial. Su propósito es permitir al cliente ver sus productos cuentas de ahorro, CTS y créditos y realizar consultas de sus saldos y movimientos.

- **Clave Dinámica Digital (CDD)**

Es un mecanismo seguro de autenticación que el Banco de la Nación pone a tu disposición y que permite recibir una Clave Dinámica Digital de ocho (08) dígitos en el dispositivo móvil seguro afiliado y sirve para confirmar las operaciones en los canales digitales. La CDD se encuentra disponible solo en territorio nacional.

- **Cliente**

Es una persona física o jurídica que ha establecido una relación formal con el Banco de la Nación. Al convertirse en cliente, la persona o entidad tiene acceso a una variedad de servicios y productos financieros proporcionados por el Banco.

- **Cifrado de Datos en Tránsito**

Implica asegurar los datos cuando se "mueven" o "transitan" a través de diversas redes o sistemas de información, mediante protocolos de cifrado y canales de comunicación seguros.

- **Cifrado de Datos en Reposo**

Implica asegurar los datos cuando se almacenan o archivan, mediante cifrado de información y control de acceso.

- **Cuentas BN**

El Banco de la Nación cuenta con los siguientes tipos de cuenta de ahorros:

- Cuenta de ahorros en agencias UOB
- Cuenta de ahorros del sector público en Moneda Nacional (MN) y Moneda Extranjera (ME)
- Cuentas de ahorros del sector privado en Moneda Nacional (MN)
- Cuenta Corriente de Detracciones
- Cuenta corriente en agencias UOB
- Cuenta corriente para proveedores del estado
- Cuentas Corrientes para asociaciones de pescadores
- Cuenta de Depósitos a plazo en Agencias UOB
- Cuenta DNI

- **DNS**

Sistema de Nombres de Dominio (Domain Name System)

- **Entidad Financiera**

Según el Banco Central de Reserva del Perú (BCRP), una entidad financiera se define como cualquier institución autorizada por la Superintendencia de Banca, Seguros y AFP (SBS) para realizar operaciones de intermediación financiera, tales como captación de depósitos, otorgamiento de créditos, emisión de valores, entre otras actividades relacionadas con el sistema financiero. Las entidades financieras pueden incluir Bancos comerciales, financieras, cooperativas de ahorro y crédito, cajas municipales, entre otras instituciones similares reguladas por la SBS.

- **Entregables**

Son productos, servicios o resultados específicos que el Contratista o se compromete a entregar en una fase determinada del proyecto.

- **Gbps**

Gigabit por segundo (Gigabit per second)

- **Hitos**

Son puntos de referencia o eventos clave que marcan el progreso del proyecto. Los hitos están vinculados a la finalización exitosa de un conjunto de entregables.

- **IOPs**

Operaciones de Escritura y Lectura (Input/Output Operations Per Second)

- **iSCSI**

Es un estándar que permite el uso del protocolo SCSI (Small Computer System Interface) sobre redes TCP/IP

- **ISO**

Organización Internacional de Normalización (International Organization for Standarization)

- **JSON**

Java Script Object Notation

- **Modelo de Entrega Servicios Cloud (Nube)**

La nube pública deberá cumplir con las siguientes características:

- ✓ **Acceso por Internet en su totalidad**: como servicio en una nube pública, el acceso a este será vía Internet, permitirá tener acceso desde cualquier ubicación siempre que se esté conectado a la red. En lo referente a la seguridad de esta conexión, dependiendo del servicio, el Contratista ofrecerá herramientas para garantizar la comunicación segura (certificados, VPN, SSH, etc.).
- ✓ **Niveles de disponibilidad de los servicios**: La nube pública, nativamente ofrece altos niveles de disponibilidad y los mismos se pueden mejorar por medio de distribuir la plataforma en varias ubicaciones.
- ✓ **Flexibilidad en el servicio**: el servicio en una nube pública ofrece de manera nativa un modelo de flexibilidad, lo que quiere decir que si este servicio necesita crecer o decrecer lo puede realizar de manera automática.
- ✓ **Sin contrato de permanencia**: Los servicios de nube pública no establecen permanencia en sus servicios, dado que el uso será totalmente por demanda, por lo que solo se utilizará durante el periodo que así lo requiera la Entidad y podrá ser dado de baja en cualquier momento.
- ✓ **Interface de administración y programación**: La nube pública ofrecerá una interface de administración del servicio adquirido. Adicionalmente habrá una plataforma para integrar distintos elementos; es decir, el Proveedor de Servicios en la Nube (PSN) debe contar con un API (interface de programación de aplicaciones o Application Programming Interface) para que este servicio pueda ser integrado o automatizado según la necesidad.
- ✓ **Soporte**: Una nube pública ofrece programas de socios que se certifican a nivel organización en los distintos niveles en función de su compromiso y experiencia con el Proveedor de Servicios en la Nube (PSN) pública, estos socios son compañías de servicios profesionales que ayudan a los clientes a dar soporte, diseñar, proyectar, crear, migrar y administrar sus cargas de trabajo y aplicaciones a/en la nube pública.
- ✓ **Conocimiento**: Una nube pública ofrece un programa de capacitación y certificación al público en general que desee obtener una certificación del conocimiento y experiencia de la nube pública.

- **NFS**

Sistema de Archivos de Red (Network File System)

- **Over the Air (OTA)**

Se refiere a varios métodos de distribución de software nuevo, configuraciones de

configuración e incluso la actualización de claves de cifrado en dispositivos.

- **OnPremise**

El software instalado localmente (a veces abreviado como "on-prem") se instala y se ejecuta en computadoras de la organización que utiliza el software, en lugar de en una instalación remota como una granja de servidores o una nube.

- **UOB**

Las personas naturales y jurídicas tienen la posibilidad de abrir su cuenta de ahorros en el Banco de la Nación (BN) y beneficiarse de los servicios de depósitos, retiros, consultas y convenios que ofrece el banco en aquellas localidades donde son la Única Oferta Bancaria (UOB).

- **Contratistas**

A continuación, se describen los Contratistas que interactuarán en la provisión de servicio requerido por la Entidad:

✓ **Proveedor de Servicios de Nube (PSN)**

El PSN se refiere al fabricante de la plataforma de servicios de nube que ofrece potencia de cómputo, almacenamiento de bases de datos, entrega de contenido y cualquier otra funcionalidad a nivel de infraestructura entregada en los diferentes modelos descritos (IaaS, PaaS y SaaS) a través de centros de datos geográficamente separados uno de otro, siendo los propietarios y responsables del mantenimiento de los equipos conectados en red que son necesarios para proveer los servicios de nube de manera pública, mediante un esquema de auto servicio.

✓ **Proveedor de Servicios – CONTRATISTA**

La solución requerida por la Entidad, así como todos los componentes y servicios que forman parte de este anexo, serán asignados a un solo Contratista de servicios, el cual suscribirá un contrato de servicios que garantice la continuidad operativa y la mejora de desempeño de la solución, de una manera segura, asequible y con la flexibilidad de poder crecer y decrecer de acuerdo a la demanda de captura y procesamiento de información. Dicho Contratista de servicios deberá estar acreditado como un Partner de negocio del PSN.

- **Titular de Cuenta**

Persona natural o jurídica que posee una cuenta en el Banco.

- **Tipos de Servicios**

Existen tres modelos fundamentales que junto a sus combinaciones derivadas describen los tipos de prestación de los servicios que cabe realizar a través de la nube.

Habitualmente, y de manera genérica, se hace referencia a esos tres modelos fundamentales como el "Modelo SPI," donde "SPI" hace referencia a Software, Plataforma e Infraestructura ("As a Service", o "como Servicio"), respectivamente,

y se definen del siguiente modo:

- ✓ **Software como Servicio (SaaS)**

Se caracteriza por la puesta a disposición de un software ofrecido como un servicio bajo demanda que se utiliza de forma compartida con otros usuarios, lo cual implica que un solo software que reside en la infraestructura del PSN puede ser utilizado por múltiples organizaciones empresariales o clientes.

- ✓ **Plataforma como Servicio (PaaS)**

Se trata de una plataforma computacional que permite el desarrollo de aplicaciones más rápida y fácilmente y sin la complejidad de comprar y dar mantenimiento al software e infraestructura que soporta a la plataforma. En estas plataformas, la ventaja que se proporciona al cliente, básicamente, consiste en poner a su disposición lenguajes y herramientas de programación que son gestionadas por el prestador de servicios.

- ✓ **Infraestructura como Servicio (IaaS)**

Tiene como principal característica el servir como medio para alcanzar capacidad tanto de procesamiento informático como de almacenamiento de información a través de servicios estandarizados prestados a través de Internet de forma que el cliente puede desplegar y ejecutar software de cualquier tipo, ya sean sistemas operativos o software propietario.

- **Token Físico**

Es un mecanismo de seguridad, consistente en una clave secreta de acceso que se actualiza cada cierto tiempo y que puede ser visualizada por el cliente en su token (dispositivo físico entregado por el Banco).

- **Respaldos**

Es una copia de seguridad - o el proceso de copia de seguridad - con el fin de que estas copias adicionales puedan utilizarse para restaurar el original después de una eventual pérdida de datos parcial o total.

- **Sistema de Geolocalización**

Solución tecnológica que determina la ubicación (dirección física) de un objeto en un entorno físico o virtual; con la capacidad de rastrear el paradero de un dispositivo utilizando GPS, torres de teléfonos celulares, puntos de acceso WiFi o una combinación de estos. La geolocalización utiliza sistemas de posicionamiento para rastrear el paradero de un individuo hasta coordenadas de latitud y longitud.

- **Saldo**

El saldo de una cuenta bancaria es la cantidad de dinero disponible en esa cuenta en un momento específico. Este saldo puede ser positivo, si hay fondos suficientes para cubrir las transacciones y deudas asociadas a la cuenta, o negativo en el caso de cuentas con sobregiros o líneas de crédito asociadas.

- **Saldo Actual**

Es la cantidad de dinero en la cuenta en el momento actual, teniendo en cuenta todas las transacciones ya registradas.

- **Saldo Disponible**

  Representa la cantidad de dinero que está realmente disponible para el titular de la cuenta, teniendo en cuenta las transacciones pendientes, cheques no cobrados y otras retenciones.

- **Saldo Contable**

  Es el saldo que el Banco considera oficial, teniendo en cuenta todas las transacciones registradas, incluso aquellas que aún no se han reflejado en el extracto de la cuenta.

- **Serverless**

  Permite crear y ejecutar aplicaciones y servicios sin preocuparse de los servidores.

- **Single-tenant**

  Es instancia que se ejecuta en una nube virtual privada (VPC) en hardware dedicado para un único cliente.

- **Snapshots**

  Copia de seguridad de los datos contenidos en los volúmenes de almacenamiento tomando instantáneas en un momento determinado.

- **Sistema Bancario**

  También conocido como sistema central, sistema o Core bancario, es una plataforma tecnológica integral que gestiona y coordina las operaciones fundamentales de un Banco. Este sistema constituye el núcleo central de las operaciones bancarias, proporcionando soporte para diversas funciones críticas, tales como:

  - **Gestión de Cuentas**: Administra la información de las cuentas de los clientes, incluyendo saldos, transacciones, historial y otros detalles relevantes.
  - **Procesamiento de Transacciones**: Facilita la ejecución y registro de transacciones financieras, como depósitos, retiros, transferencias, pagos y otros movimientos.
  - **Gestión de Préstamos**: Administra la información relacionada con préstamos, incluyendo tasas de interés, plazos, amortizaciones y otros aspectos asociados a los productos crediticios.
  - **Seguridad y Cumplimiento**: Garantiza la seguridad de la información confidencial y asegura el cumplimiento de regulaciones y normativas bancarias.

- **Contabilidad y Reportes**: Realiza el seguimiento contable de todas las operaciones, generando informes financieros y estadísticas para la toma de decisiones.
- **Integración con Canales**: Se integra con diversos canales de atención al cliente, como aplicaciones móviles, banca en línea, cajeros automáticos y otros puntos de contacto.
- **Gestión de Riesgos**: Evalúa y controla los riesgos asociados a las operaciones bancarias, incluyendo la evaluación de créditos y la gestión de riesgos financieros.

- **Transferencia Bancaria**

  Una transferencia bancaria es el movimiento de fondos electrónicos de una cuenta bancaria a otra. Este proceso permite a los individuos y empresas enviar dinero de una entidad financiera a otra de manera rápida y segura. Las transferencias bancarias pueden realizarse dentro del mismo Banco (transferencia interna) o entre Bancos diferentes (transferencia interbancaria) y pueden ser de manera inmediata o diferida.

- **TLS**

  Seguridad de la capa de transporte

- **Usuario**

Se refiere a una persona o entidad que utiliza los servicios y productos proporcionados por una institución bancaria sin haber establecido una relación formal con una institución bancaria.

- **Servicio de Mensajes Cortos (Short Message Service SMS, en inglés)**

SMS son las siglas en inglés de "Short Message Service", que en español se traduce como "Servicio de Mensajes Cortos". Es un servicio de comunicación que permite el intercambio de mensajes de texto entre dispositivos móviles, como teléfonos móviles o, en algunos casos, sistemas fijos. Los mensajes de texto enviados a través de SMS suelen tener un límite de caracteres, generalmente 160 caracteres por mensaje.

- **ME**

Moneda Extranjera

- **MN**

Moneda Nacional

- **Notificaciones PUSH**

Las notificaciones push son mensajes o alertas que se envían directamente a un dispositivo móvil desde una aplicación o servicio, incluso cuando la aplicación no está activa. Estas notificaciones se utilizan para informar a los usuarios sobre

eventos importantes, actualizaciones, mensajes o cualquier otra información relevante.

- **QR "Quick Response"**

Es un código de respuesta rápida. Es la evolución del código de barras y permite, al ser escaneado, ver la información que contiene. Entre otras aplicaciones de este código de barras, el código QR es usado frecuentemente para facilitar los pagos en línea desde el celular de forma rápida y sin la necesidad de manipular dinero.

- **WAF**

Firewall de Aplicaciones Web (Web Application Firewall)

- **VPN**

Red privada virtual

5. BASE LEGAL Y NORMATIVA

La ejecución del servicio debe realizarse dentro del marco de las siguientes normas peruanas o leyes aplicables según corresponda:

- Ley N° 29733 – Ley de protección de datos personales
- Decreto Legislativo N° 1412-2018 - Decreto Legislativo que aprueba la Ley de Gobierno Digital.
- Decreto Supremo N.º 050-2018-PCM - Decreto que establece la definición de Seguridad Digital de ámbito nacional, en el cumplimiento con la Segunda Disposición Complementaria Final de la Ley N°30618, Ley que modifica el Decreto Legislativo N°1441.
- Decreto Supremo N.º 029-2021-PCM - Decreto Supremo que aprueba el Reglamento de la Ley de Gobierno Digital
- Decreto Supremo N° 085-2023-PCM - Decreto Supremo que aprueba la Política Nacional de Transformación Digital al 2030
- Resolución SBS N° 504-2021 – Aprueba el reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad.
- Resolución SBS N° 6523-2013 y sus modificatorias – Reglamento de Tarjetas de Crédito y Débito.
- Directiva BN-CIR-2100-216-05 Gestión de riesgos de nuevos productos o cambios importantes en el ambiente de negocios, operativo o informático del Banco
- Directiva BN-MAN-2100-010-06 Manual para el tratamiento de las contrataciones / subcontrataciones significativas en el Banco de la Nación
- Directiva BN-DIR-7700-272-03 Gestión del Portafolio y Proyectos.
- Directiva BN-DIR-8300-147-01 Ciclo de Vida del Software
- Directiva BN-DIR-5500-152-01 Contratación de Servicios Financieros en el BN
- Directiva BN-DIR-2400-112 Gestión de claves criptográficas

6. OBJETIVO DE LA CONTRATACIÓN

6.1. Objetivo General

Implementar los canales digitales Banca Móvil y Banca por Internet del Banco de la Nación con un enfoque orientado a mejorar la experiencia del cliente.

6.2. Objetivos Específicos

i Contar con un canal de fácil acceso, intuitivo y robusto para los clientes.
ii Promover el uso de los canales digitales.
iii Incrementar los clientes y las operaciones digitales.

6.3. Vinculación del Objetivo con la Meta del PEI

El presente requerimiento se encuentra relacionado a los siguientes Objetivos Estratégicos Institucionales del Plan Estratégico Institucional PEI 2022- 2026:

Objetivo Operativo 05: Masificar el acceso y uso de los canales alternos, que permitirá alcanzar el objetivo operativo: Migración de operaciones en canales alternos.

Objetivo Operativo 06: Incrementar las operaciones y los clientes digitales, que permitirá alcanzar el objetivo operativo: Incremento de operaciones en canales digitales.

7. ALCANCE Y DESCRIPCIÓN DEL SERVICIO

7.1. Descripción y Condiciones del Servicio

El presente proyecto de la nueva plataforma de los canales digitales del Banco de la Nación tiene como alcance principal la modernización y optimización de la Banca Móvil y la Banca por Internet. Se busca mejorar la experiencia del usuario, asegurar el consumo eficiente de los recursos de Nube (procesamiento, seguridad, ejecución de APIs, entre otros componentes) y cumplir con las demandas tecnológicas actuales del mercado. Para alcanzar este objetivo, se contempla la incorporación de diversos mecanismos tecnológicos disponibles en el mercado actual. Estos elementos respaldarán los volúmenes de transacciones financieras y no financieras que se llevarán a cabo a través de estos canales digitales.

El servicio considera la contratación de un Contratista para el desarrollo e implementación de la nueva plataforma de los canales digitales: Banca Móvil y Banca por Internet, del Banco de la Nación. Así como el desarrollo de las APIs correspondientes, de acuerdo con los siguientes aspectos generales:

a El presente proyecto se desarrollará e implementará de acuerdo al Documento Normativo BN-DIR-7700-272-03 Rev 4.0 de Gestión del Portafolio y Proyectos, el cual establece el marco de gobernanza para la gestión de portafolio y proyectos. El proyecto contempla una metodología

tradicional para el desarrollo de las soluciones (Banca Móvil y Banca por Internet), el cual se basa en 14 entregables (ver numeral 16. Entregables). El contratista podrá utilizar algunas ceremonias ágiles, previo conocimiento y aprobación del área usuaria, de ser necesario (modelo hibrido). Además, para el servicio de Mejora Continua (ver numeral 33. Servicio de Asistencia para Alcanzar Mejora Continua de la Solución), será bajo el enfoque de Metodologías Ágiles, según normativa del Banco.

b El Product Backlog correspondiente a los canales digitales de Banca Móvil y Banca por Internet del Banco de la Nación, el cual detalla las funcionalidades y requisitos del proyecto, se encuentra especificado en el Anexo N° 1 del presente documento.

c Como parte de la implementación, se espera que el Contratista elabore y presente como mínimo dos (02) propuestas para la Banca Móvil y dos (02) propuestas para la Banca por Internet, que incluyan: la maquetación (mockups) y los diseños de interfaces tomando en consideración los principios[3] de diseño centrado en la experiencia del usuario (UX/UI). Estas propuestas deberán ser sometidas a la aprobación de las áreas involucradas y de los responsables correspondientes del Banco. Asimismo, el Contratista deberá respetar la línea gráfica según corresponda el manual de marca del Banco de la Nación, que será provisto por el Banco, a través del área usuaria.

d El Contratista deberá implementar la capacidad de diseño web responsivo para la Banca por Internet del Banco de la Nación, asegurando que la interfaz se adapte de manera óptima a diferentes dispositivos y tamaños de pantalla.

e En la nueva versión de los canales digitales del Banco de la Nación, es importante adoptar un enfoque de comunicación sencilla, simple, directa y cercana, evitando el uso excesivo de tecnicismos.

f En la nueva versión de los canales digitales del Banco de la Nación, se enfatiza la importancia de emplear iconografía de manera destacada sobre el texto. Es decir, esta estrategia busca favorecer el reconocimiento visual antes que la lectura, mejorando la experiencia del usuario al facilitar la comprensión rápida y eficiente de las funciones y servicios disponibles[4].

g La implementación de la plataforma de Banca por Internet debe cumplir con los estándares y prácticas de desarrollo web vigentes a fin de asegurar su correcta visualización y optimización en los principales motores de navegación o de renderización del mercado[5] (WebKit, Blink, Gecko).

h La nueva versión de la aplicación móvil del Banco de la Nación deberá garantizar una experiencia nativa en dispositivos Android (versión 8.0 o superior) e iOS (versión 14.3 o superior). Además, el paquete de la

[3] Design Toolkit | Principios. (s. f.). http://design-toolkit.uoc.edu/es/category/principios/
[4] Informe de resultados – Servicio de experiencia de Usuario (UX/UI)
[5] Browser market share worldwide | StatCounter Global Stats. (s. f.). StatCounter Global Stats. https://gs.statcounter.com/browser-market-share

aplicación deberá ser publicado en las tiendas de aplicaciones móviles de AppStore (Apple), PlayStore (Google) y AppGallery (Huawei). Se precisa que la Banca por Internet implementada deberá comunicarse en línea con los sistemas bancarios.

i Es responsabilidad del Contratista garantizar la correcta integración de las nuevas versiones de la Banca Móvil y la Banca por Internet con los sistemas financieros, no financieros y con los sistemas antifraude para las distintas operaciones financieros y no financieros del Banco de la Nación (la integración con los sistemas antifraudes deberá ser completadas y entregadas al concluir el MVP 1).

j El Contratista deberá asegurar que los datos generados en la nueva plataforma del Canal Digital (Banca Móvil y Banca por Internet) se registren de manera íntegra en las bases de datos de los sistemas actuales. Todas las adecuaciones necesarias para que estos datos sean incorporados a las bases de datos actuales del Banco será responsabilidad del Contratista.

k La información generada por las operaciones en los canales digitales, tanto la Banca Móvil como la Banca por Internet, se registrará como eventos de comportamiento de los usuarios en los LOGs de la aplicación y almacenará en la base de datos compatibles con MongoDB y PostgreSQL. Estos registros estarán disponibles durante un periodo mínimo de 30 días calendarios para consulta y análisis. Además, el Contratista diariamente colocará los datos cada 24 horas en un repositorio definido por el Banco que le permitirá migrarlos a un entorno on-Premise. El Contratista deberá desarrollar una consulta que permita visualizar los datos, considerando los filtros necesarios para una adecuada lectura de los mismos, asimismo, debe permitir de descarga de los datos en formato CSV. Esta consulta debe estar disponible para ser integrada en el aplicativo de consultas de BancaMóvil-MWBM. La solución debe incluir una función de consulta del registro de sucesos (LOG) de los canales de Banca Móvil y Banca por Internet. Este registro debe ser accesible a través del monitor implementado por el Banco. Además, se debe garantizar que esta consulta esté disponible para su integración en las aplicaciones del Banco.

l El Contratista deberá cumplir con todas las funcionalidades necesarias para satisfacer los requerimientos del negocio del Banco, así como con cualquier otro aspecto que la entidad bancaria esté obligada a cumplir. Esto incluye tanto las funcionalidades específicas solicitadas por el Banco como cualquier requisito adicional necesario para garantizar el cumplimiento de las obligaciones y regulaciones pertinentes. El Contratista deberá asegurar que la solución proporcionada cumpla con todos estos requisitos de manera integral y efectiva.

m El Contratista deberá garantizar el uso de los mecanismos para una comunicación (APIs) con el Core bancario del Banco de la Nación y otras

entidades financieras[6] reconocidas por el Banco Central de Reserva del Perú (BCRP), empresas de servicios u otras que defina el Banco y que cuenten con convenios vigentes durante el desarrollo del presente proyecto. El Banco se integra con las entidades financieras a través del servicio de interoperabilidad con la Cámara de Compensación Electrónica (BCRP) y el sistema LBTR. Asimismo, el Banco cuenta con 2 tipos de integraciones: transferencias inmediatas de bajo monto (interoperabilidad) y de alto monto (LBTR). Finalmente, se espera que la nueva plataforma mantenga el tiempo de carga de páginas y tiempos de respuesta de dos (02) segundos. Este tiempo no incluye los tiempos de respuesta de las entidades externas[7].

n Durante la prestación del servicio, el Contratista se compromete a garantizar la implementación de las normativas vigentes emitidas por los entes reguladores que son de obligatorio cumplimiento por parte del Banco.

o La nueva plataforma de Banca Móvil y Banca por Internet debe permitir la parametrización de configuraciones a fin de adaptar la plataforma a sus necesidades específicas. Las configuraciones parametrizables se pueden gestionar desde el backend de la plataforma por parte del personal autorizado del Banco. Esto permite al Banco realizar cambios en la configuración sin necesidad de realizar una nueva implementación de la plataforma (ver numeral 7.13 Módulo de administración).

p El Contratista deberá asegurar que la solución implementada proporcione cifrado de datos en tránsito y cifrado de datos en reposo, con el fin de prevenir el acceso no autorizado a información restringida por parte de usuarios no autorizados. Asegurar el uso de algoritmos criptográficos sólidos y la gestión de claves criptográficas seguras, para proteger la confidencialidad, autenticidad e integridad de la información de los clientes que se transmite entre el BN con las entidades públicas, proveedores y canales digitales; de acuerdo a los lineamientos establecidas en la directiva BN-DIR-2400-112 Gestión de claves criptográficas.

q El Contratista deberá asegurar y garantizar que los datos estén protegidos por medidas de seguridad organizativas, administrativas y técnicas adecuadas para preservar la confidencialidad de la información personal (ver numeral 37. Seguridad de la Información y Ciberseguridad)

r El Contratista deberá cumplir con las medidas de seguridad organizativas de acuerdo a la Ley N.° 29733 Ley de Protección de Datos Personales, referente al derecho de información en el cual el Contratista debe informar la finalidad específica para el tratamiento de los datos personales de los clientes.

[6] Entidades Financieras. (s. f.). https://www.bcrp.gob.pe/sitios-de-interes/entidades-financieras.html
[7] *Pliego de Consultas N° 01-2024 - Concurso de Méritos (Consulta N° 3 PERÚ APP).*

s Los siguientes servicios serán proporcionados por el Banco de la Nación para la aplicación móvil y Banca por Internet a fin de que el contratista pueda disponer o integrarse:

i Clave Dinámica Digital:

El Banco, mediante su área técnica, gestionará el servicio de generación de Clave Dinámica Digital o token digital con el fin de autenticar al dispositivo y las transacciones, tanto financieras como no financieras (según necesidad), llevadas a cabo a través de los canales digitales.

ii Servicios de Biometría Facial:

El Banco proporcionará los parámetros técnicos para establecer la comunicación de manera correcta con el servicio de la identificación de los clientes.

iii Membresía de las Tiendas de Aplicaciones para Android (Google Play), iOS (App Store) y AppGallery (Huawei):

Registro y presencia en las tiendas de aplicaciones para Android y iOS para facilitar la distribución y actualización de la aplicación.

El Banco cuenta con la autorización de los fabricantes a fin de cargar los archivos necesarios para la publicación y distribución de las aplicaciones mediante sus tiendas de aplicaciones.

iv Protocolo de Seguridad para Cifrado (Secure Sockets Layer – SSL):

El Banco proporcionará los Certificados de Seguridad tipo SSL.

v Traducción en idioma quechua

El Banco brindará al Contratista los términos traducidos en idioma quechua para la aplicación móvil y Banca por Internet.

vi Manual de Marca Institucional

El Banco brindará el manual de marca institucional donde se encuentra la línea gráfica.

vii Sistema antifraudes

El Banco brindará el acceso a sus servicios antifraudes, los cuales deberán ser integrados por el Contratista en la solución propuesta.

viii Cuenta DNI

En el caso de consumir los servicios del Nube

ix Servicios externos

Chat Bot, Págalo, Mesa de ayuda (enlaces externos)

t El Contratista será responsable de suministrar la información necesaria a los sistemas y/o bases de datos del Banco ya existentes, siguiendo el formato de archivo que el Banco indique en la etapa de análisis y diseño del Ralease I del proyecto, para la generación de por lo menos 20 reportes regulatorios, mandatorios u operativos de las transacciones que se realicen en los canales digitales.

u El Contratista deberá asegurar que el Punto Objetivo para Recuperación (POR) será de cero para las transacciones financieras.

v El Contratista deberá asegurar que el Tiempo Objetivo para Recuperación (TOR) será de cinco (05) minutos por incidencia.

w El alcance del presente proyecto involucra a todas las cuentas pasivas (Cuenta de ahorros en agencias UOB, Cuenta de ahorros del sector público en MN y ME, Cuentas de ahorros del sector privado en MN, Cuenta Corriente de Detracciones, Cuenta corriente en agencias UOB, Cuenta corriente para proveedores del estado, Cuentas Corrientes para asociaciones de pescadores, Cuenta de Depósitos a plazo en Agencias UOB, Cuenta DNI en HOST) que se encuentre disponibles en el Core bancario, desde el MVP 1.

x La solución incluya una de consulta del LOG de uso de los canales Banca Móvil y Banca por Internet y que debe estar disponible en el monitor de la aplicación, además se debe mencionar que esta consulta debe estar disponible para ser integrada a las aplicaciones por parte del Banco.

y La implementación de la nueva plataforma de Banca Móvil y Banca por Internet debe cumplir con los estándares actuales del mercado, integrando las mejores prácticas en seguridad y desarrollo de software. Además, en caso de utilizar librerías, metodologías, frameworks y patrones de diseño de software, estos deben ser seleccionados cuidadosamente a fin de asegurar la eficiencia y calidad de los productos finales, previo conocimiento del área técnica del Banco.

z Del punto anterior, en caso de considerar el uso de software libre (Open Source), el contratista deberá garantizar el soporte necesario. Si el contratista adquiere alguna librería propietaria para el funcionamiento de la Banca Móvil y la Banca por Internet, esta deberá ser adquirida a nombre del Banco de la Nación. El costo de estas librerías deberá estar incluido en los costos totales de desarrollo e implementación de la nueva plataforma de los Canales Digitales del Banco de la Nación y no será sujeto a pagos adicionales. Una vez finalizado el contrato, el Banco mantendrá la licencia de uso, administración y control de dichos componentes. En ambos casos, el contratista deberá proporcionar, al finalizar cada MVP, un informe detallado y un manual de instalación sobre los componentes de software utilizados, incluyendo las versiones correspondientes.

7.2. Enrolamiento al Canal Digital

Generación de Clave de Internet y Clave Dinámica Digital (CDD)

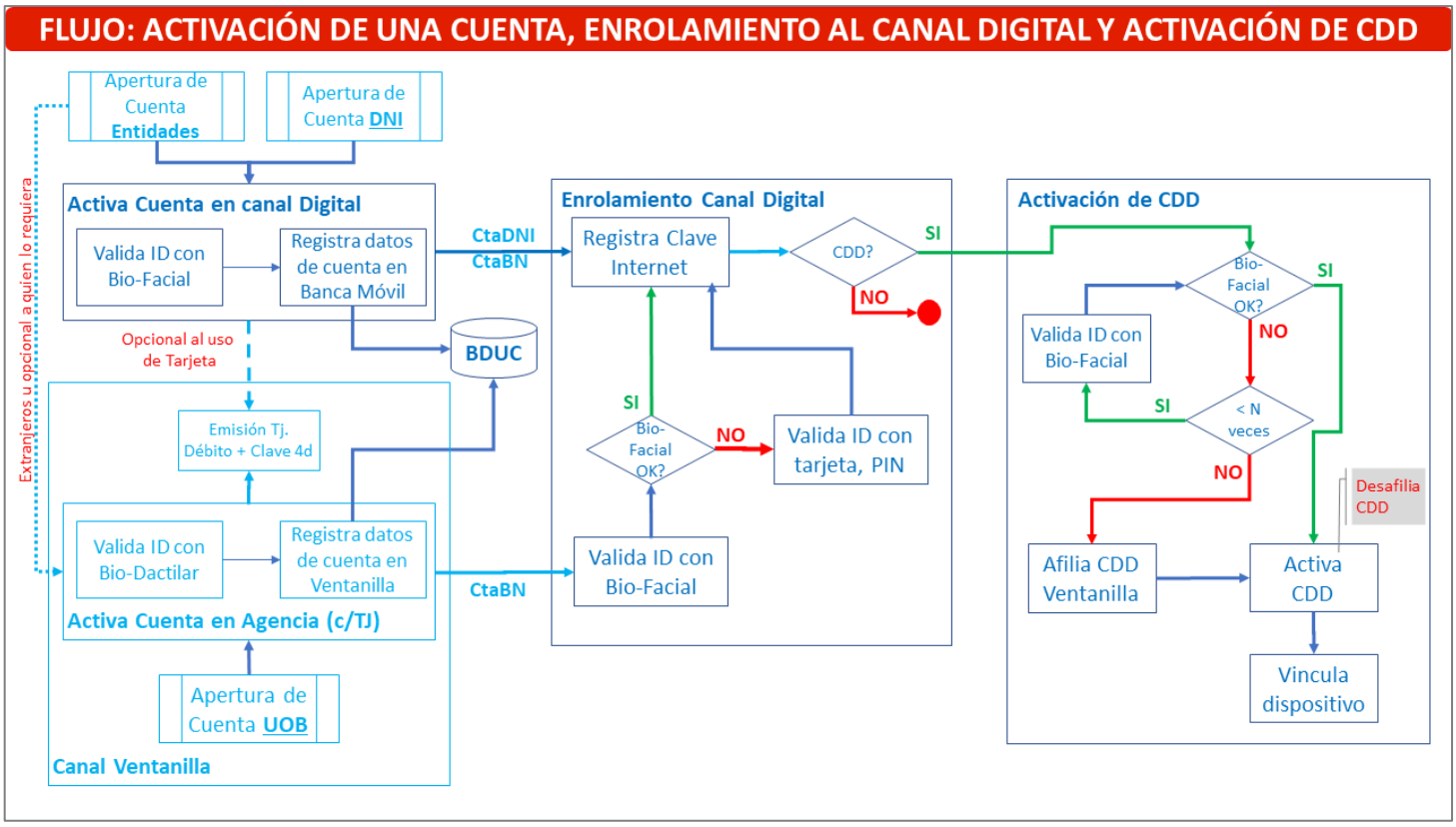


Ilustración 1: Flujo de activación de una cuenta, enrolamiento al canal digital y activación de CDD (Diagrama referencial)

Fuente: Banca Digital – Subgerencia de Innovación Digital

a Consideraciones Generales

i El proceso de enrolamiento a los canales digitales del Banco de la Nación permite a los clientes generar su clave de acceso con la que podrá autenticarse de manera segura en los canales Banca Móvil y Banca por Internet del Banco.

ii Durante este proceso, los clientes deberán validar su identidad con los mecanismos de seguridad implementados por el Banco:

- **Clientes con cuenta de ahorros tradicional**: validación de identidad con Tarjeta, PIN de la tarjeta, número del DNI y fecha de nacimiento.
- **Clientes con cuenta digital (Cuenta DNI)**: validación de identidad con biometría.

iii La generación de la clave de acceso permite al cliente acceder a los canales digitales donde estarán disponibles los productos pasivos que tiene el cliente con el Banco (Cuenta de ahorros, Cuenta DNI, cuenta corriente, CTS, préstamos, entre otros). El acceso al canal es en modo de consulta, para poder realizar operaciones financieras o actualizar sus datos, es necesario que el cliente se afilie a la Clave Dinámica Digital (CDD).

iv Para la Banca Móvil, al finalizar el proceso de enrolamiento, se ofrecerá al cliente la posibilidad de asociar su inicio de sesión con

mecanismos propios de seguridad proporcionados por los fabricantes de teléfonos, tales como reconocimiento facial (FaceID en caso de Apple) o huella dactilar para Android. Valida que la biometría facial esta activa, en caso contrario, la aplicación deberá solicitar al cliente verificar su identidad por biometría facial.

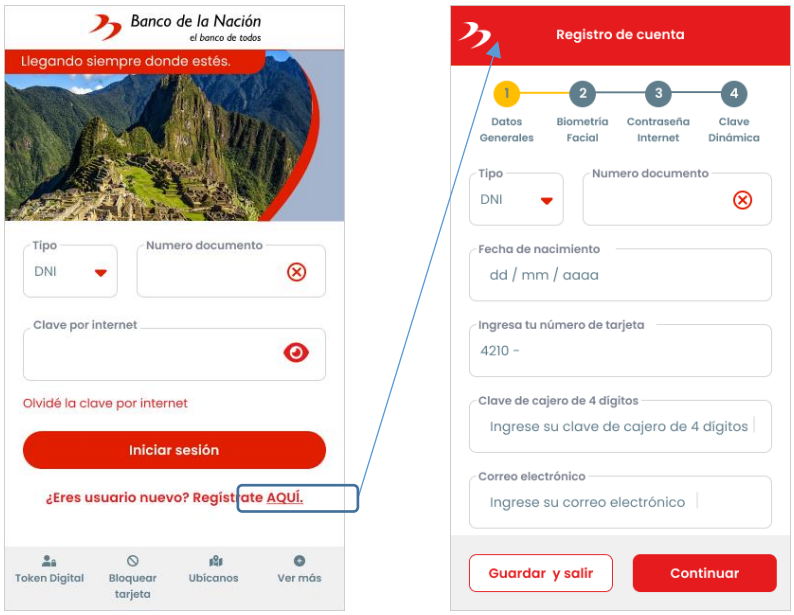


Ilustración 2: Acceso desde la aplicación móvil (imagen referencia)

Fuente: Banca Digital – Subgerencia de Innovación Digital

v Si el proceso de generación de la clave de acceso se lleva a cabo a través del canal Banca Móvil, se procederá luego con una consulta al cliente sobre su interés en afiliarse a la Clave Dinámica Digital (CDD). La decisión de activar o no la CDD para realizar operaciones financieras desde los canales digitales quedará a discreción del cliente.

vi Después de que el cliente haya completado el proceso de registro, la primera pantalla que se presentará será la pantalla de Login o inicio de sesión.

b Descripción del Proceso de Enrolamiento a los Canales Digitales

i El ciudadano inicia la aplicación móvil o Banca por Internet del Banco de la Nación y elige la opción "Genera tu clave de Internet" o función similar.

ii A continuación, el ciudadano selecciona su tipo de documento de identidad (DNI, Canet de extranjería o Pasaporte) e ingresa su número de documento.

iii Valida si el ciudadano tiene una Cuenta BN

- El sistema verifica si el documento registrado pertenece a un cliente y si posee una cuenta de ahorros tradicional activa.
- Si el cliente dispone de una cuenta de ahorros activa, pero aún no ha generado su clave de Internet, el sistema lo dirigirá al "Proceso de generación de clave de acceso a los canales digitales".
    - El cliente debe tener al menos una tarjeta de débito contratada con el Banco.
    - Está disponible para clientes con tipo de documento DNI
    - Validación de identidad del cliente
        - Registra número de la tarjeta de débito.
        - Registra la clave de la tarjeta de cuatro (04) dígitos y valida que la clave corresponda a la tarjeta registrada.
        - Registra su tipo y número de documento y valida que el documento corresponda al titular de la tarjeta registrada.
        - Registra la fecha de nacimiento y valida que corresponda con el documento registrado.
        - Si los datos son conformes, continúa con el registro de la clave de internet.
    - Registra clave de internet
        - Registrar la clave de internet
        - Confirmar la clave de internet
        - Aceptar los Términos y Condiciones para generar la clave de internet.
        - Se registra la Clave de Acceso en una base de datos centralizada. Ver numeral 7.5 Gestión de Claves Centralizadas.
        - Registra estado de Clave de Acceso:
            - Con clave de acceso
            - Sin clave de acceso.
    - Se genera la constancia de Generación de Clave de Internet
    - Mostrar en pantalla la constancia de Generación de Clave de Internet, incluyendo la funcionalidad de compartir.
    - El cliente tendrá la opción de generar su Clave Dinámica Digital CDD o podrá desestimarlo y generarla cuando considere oportuno.
    - Cuando el servicio de biometría facial incluya la integración con Migraciones, se incluirán a clientes con tipo de documento pasaporte o carné de extranjería. Mientras tanto, los clientes extranjeros deberán realizar el trámite de la afiliación de manera presencial en las agencias del Banco de la Nación, según el procedimiento vigente.
- En caso de que el cliente ya disponga de una clave de acceso, se indicará al cliente que puede realizar el cambio de esta, ingresando

a la aplicación o Banca por Internet en la opción de "Cambio de Clave de Acceso" o función similar que determine el Banco.

- Si el ciudadano no tiene una cuenta de ahorros activa, el sistema lo deriva al proceso "Valida si el cliente tiene una Cuenta DNI activa".

iv Valida si el cliente tiene una Cuenta DNI activa

- Si el ciudadano no tiene Cuenta DNI, el sistema le hará la consulta para que confirme si desea realizar la apertura de su Cuenta DNI "No tienes una Cuenta DNI, confirma si deseas realizar la apertura de tu Cuenta".
    - Si el ciudadano confirma la apertura, se ejecuta el "Proceso de Apertura de Cuenta DNI" en el Core de Cuenta DNI.
    - Culminado el proceso de apertura de cuenta, se integra al proceso de "Enrolamiento a la Cuenta DNI" para que el cliente realice la activación de su cuenta.
    - Si el ciudadano no confirma la apertura, culmina el proceso y retorna a la pantalla inicial de Login.
- Si el ciudadano si tiene Cuenta DNI y esta se encuentra activa, evalúa si el cliente aún no tiene su Clave de Acceso
    - En caso de que ya disponga de una Clave de Acceso, se indicará al cliente que puede realizar el cambio de la misma, ingresando a la aplicación o Banca por Internet en la opción de "Cambio de Clave de Acceso".
    - En caso aún no tenga Clave de Acceso:
        - Valida la identidad del cliente mediante el servicio de validación de identidad con biometría facial.
        - Si la validación es conforme, el cliente debe generar su clave de internet.
        - Registra clave de internet
            - Registrar la clave de internet
            - Confirmar la clave de internet
            - Aceptar los Términos y Condiciones para generar la clave de internet.
        - Si el ciudadano si tiene Cuenta DNI y esta no se encuentra activa (pendiente de enrolamiento), se integra al proceso de "Enrolamiento a la Cuenta DNI" (ver numeral 7.3 Enrolamiento a la Cuenta DNI). Cabe señalar que el proceso de enrolamiento a la cuenta DNI culmina con la generación de la clave de internet.

7.3. Enrolamiento a la Cuenta DNI

a La Cuenta DNI es una cuenta digital que se apertura de manera automática por el Banco o a solicitud de alguna entidad del Estado. La cuenta nace inactiva y es necesario que el cliente realice la activación de su cuenta ingresando a un proceso de "Enrolamiento a la Cuenta DNI" donde se solicita al cliente que registre toda la información necesaria para la activación de su cuenta digital.

b Para acceder el proceso de enrolamiento tenemos dos escenarios o flujos a implementar:

- i Clientes que tienen una Cuenta BN, van a disponer de una opción "Activa tu Cuenta DNI" dentro de la aplicación.
- ii Clientes que no tienen una Cuenta BN, van a poder realizar la activación de su Cuenta DNI desde la opción de "Generación de la Clave de Acceso". En caso no tengan su cuenta DNI abierta, el cliente tendrá la opción de realizar la apertura de la cuenta en línea para continuar con el enrolamiento.

c El Flujo de enrolamiento a la Cuenta DNI considera cuatro subprocesos:

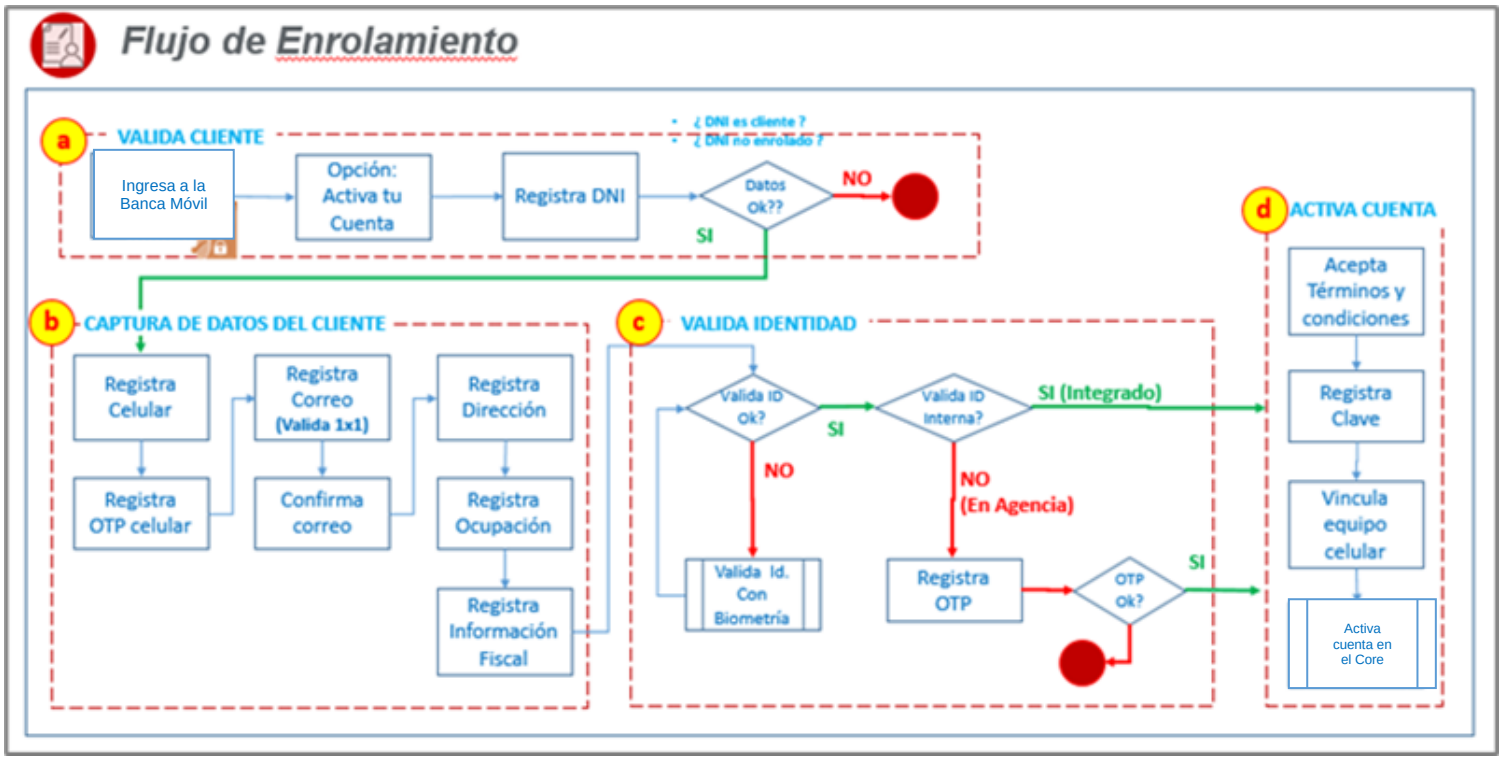


Ilustración 3: Flujo de enrolamiento a la Cuenta DNI

Fuente: Gerencia de Banca Digital - Subgerencia de Innovación Digital

- i Validación de Cliente: valida que el DNI registrado corresponda a un cliente, que no se encuentre enrolado o que se encuentre habilitado para poder re-enrolarse para que pueda continuar con la captura de datos.

ii Captura de Datos del cliente: Permite el registro de todos los datos requeridos del cliente para poder activar su cuenta.

iii Valida Identidad: Se integra con un proceso de Bio-Facial a fin de validar la identidad del cliente, en caso de no ser posible esta validación, se puede ir a una agencia a validar su identidad con Bio-Dactilar.

iv Activa Cuenta: Muestra los Términos y Condiciones de la Cuenta DNI para que el cliente pueda aceptar los mismos de manera obligatoria, opcionalmente aceptar el tratamiento de datos y con la confirmación se integra al Core bancario para ejecutar la activación de la cuenta. Luego se integra a los procesos:

- Generación de la Clave de acceso a los canales digitales.
- Afiliación a la CDD y vinculación del dispositivo seguro.

d Descripción operativa del Flujo

i Validación de Cliente

- El ciudadano debe ingresar a la Banca Móvil del BN y ubicar la opción Genera tu Clave de Acceso, donde deberá registrar su número de DNI para activar su Cuenta DNI.
- Valida si el DNI está relacionado a una cuenta en Core de cuenta DNI.
  - Si no tiene una cuenta creada en Core de cuenta DNI, consulta al cliente si desea crear su cuenta en línea
    - Si el cliente confirma, se integra con un servicio para crear la Cuenta en Core de cuenta DNI.
    - Si el cliente no confirma, cancela el proceso y lo indica con un mensaje al ciudadano.
  - Si tiene una cuenta, continúa con el proceso
- Valida si el DNI ya tiene una cuenta Enrolada
  - Si la cuenta ya se encuentra enrolada, consulta si el DNI tiene el indicador de Re-enrolamiento activo para continuar, caso contrario se muestra un mensaje al cliente indicando que ya se encuentra Enrolado.
  - Si la cuenta no se encuentra enrolada, continúa con el proceso.
- Con los datos conformes, continúa con el proceso de Captura de datos del cliente.

ii Captura de datos del cliente

- Registro de celular
  - Integración a OSIPTEL para validar titularidad (según necesidad).
    - Definir dentro del workflow una actividad para esta integración, la cual pueda ser activada o desactivada.
    - Definir una bandera para indicar si se requiere validar la titularidad del DNI con el celular.

- Definir una bandera para indicar si se requiere validar la antigüedad del contrato del celular de acuerdo a un parámetro de días (30 días por defecto).
- Si realizamos la integración a OSIPTEL y desactivamos las validaciones, esta información se debe almacenar en la solución, a fin de ser mostrada en el monitor para atención de reclamos, considerando que OSIPTEL retorna el indicador de Titularidad y una fecha de contrato del celular.
- Guardar la información recuperada de OSIPTEL en la BD de enrolados a fin de poder mostrarlos en el monitor de la aplicación.

- Envío de OTP por SMS y registro de OTP para validar tenencia del celular.
- Parametrizar tiempo de vigencia de la OTP (a nivel de Aplicación y Proceso).
- Mostrar en pantalla el tiempo de vigencia pendiente del OTP y habilitar el reenvío solo al caducar dicha vigencia.
- Valida que el número de celular sea único para la plataforma.

– Registro del correo
- Valida que el correo exista usando un servicio que valida la existencia del mismo, en caso la respuesta sea negativa, mostrar un mensaje de error indicando que el correo no es válido y que no debe usar correos corporativos.
- Valida que el correo sea único para la plataforma.
- Valida la descripción del correo con un registro doble.

– Registra la dirección del cliente, muestra por defecto los datos recuperados de RENIEC para que el cliente pueda confirmar o actualizar su dirección.
- Si la cuenta esta creada en el Core, los datos se toman de ese origen, ya que contienen toda la información entregada por RENIEC.
- Si la cuenta aún no está creada el flujo deberá considerar la consulta de datos a BDUC y/o RENIEC.

– Registra la ocupación y el RUC del cliente (en caso de contar con él) así como también su centro de labores.
- La ocupación se debe seleccionar de una lista.
- Campo para indicar si cuenta con RUC
  - El RUC se debe construir de forma automática con el DNI registrado, utilizando el módulo 11.
  - Permitir la modificación manual del mismo en caso el cliente lo requiera.
  - Validar la estructura del RUC con el módulo 11 y mostrar error en caso no cumpla con los requisitos "RUC inválido, por favor corrige tu RUC".

- El Centro de labores viene por defecto con "No declarado". Dato obligatorio, mostrar error en caso el campo se encuentre en blanco.

– Registra su información fiscal.
  - Indica su nació en Perú, por defecto marcado en Si y seleccionado Perú. De indicar No, presentar lista desplegable de países para permitir selección del país.
  - Indica si tributa en USA,
    - Por defecto marcado en No.
    - De indicar que Si,
      - Desplegar el tipo de documento: NIT (Número de Identificación Tributaria), SSN (Número de Seguridad Social), EIN (Número de identificación de empleador)
      - Desplegar un campo de texto de 20 caracteres alfanuméricos (obligatorio), para registrar el número del tipo de documento indicado.
  - Indica si tributa en otros países.
    - Por defecto marcado en No.
    - De tributar en otros países, capacidad de registrar hasta 3 países.
      - Desplegar lista de países para seleccionar.
      - Indicar si tiene número de NIT. En caso de colocar Si, permitir el registro del número de NIT (20 caracteres). En caso de indicar que No, permitir el registro de un texto libre (96 caracteres) para que el cliente indique la razón por la que no cuenta con el NIT.

– Consideraciones especiales
  - Si el cliente no culmina el registro de sus datos y sale de la sesión por cualquier motivo, el sistema debe tener la capacidad de guardar la información ya registrada para que al retornar pueda continuar.
  - El registro se podría interrumpir por diversos motivos:
    - Al no poder realizar la validación de identidad con la Biometría Facial. Lo cual lo lleva a realizar la Validación de Identidad Externa, implementada con Biometría Dactilar.
    - Al no tener el equipo que desea vincular.
    - Culmina el tiempo de la sesión definido como parámetro.

iii Valida Identidad del ciudadano

– Verifica si el DNI ya tiene el indicador de validación de identidad vigente.
  - Si no tiene validación de identidad, se integra al proceso de "Validación de identidad con Biometría Facial"
    - Dicho proceso es una caja negra que genera una respuesta de HIT o NO HIT. Ver Anexo "Servicio de Validación de Identidad con Biometría Facial"

- Si la respuesta es HIT, considerando que la validación se realizó de manera integrada, continúa con el proceso "Captura de Datos del Cliente"
- Si la respuesta es NO HIT, presenta el mensaje de error en pantalla invitando al cliente para que pueda validar su identidad de manera externa en una Agencia (validación de identidad externa) y culmina el proceso.

- Si ya tiene validación de identidad y está vigente, significa que el cliente realizó su validación de identidad de manera externa en ventanilla. En ese caso:
  - Solicita el registro de la OTP enviada al celular del cliente cuando realizó su validación externa en ventanilla.
  - Se verifica que la OTP registrada sea válida y se encuentre vigente.
  - Si la OTP es conforme, continúa con el proceso de Activación de la Cuenta.
  - Si OTP no es conforme, se muestra un mensaje al cliente "OTP inválida" y culmina el proceso.
  - Si OTP no se encuentra vigente, se muestra un mensaje al cliente "OTP no vigente" y culmina el proceso.

iv Activación de la Cuenta

- Presenta los Términos y Condiciones del contrato.
  - Solicita la confirmación de la aceptación de los T&C – obligatorio.
  - Solicita la confirmación para el tratamiento de datos – no obligatorio.
- Se integra con el Core Bancario a fin de activar la cuenta y guardar toda la información capturada. Con la confirmación del Core:
  - Envía constancia de la activación de la cuenta al correo del cliente.
  - Envía contrato de la cuenta al correo afiliado.
- Registra la Clave de Acceso de seis (06) dígitos (Clave de Internet).
  - Valida estructura de la clave.
  - Utiliza teclado dinámico.
  - Solicita confirmación de la clave con registro doble.
  - Guardar la información Cliente-Clave en un repositorio centralizado, de manera que pueda ser utilizado por otras aplicaciones que así lo requieran. Ver "Gestión de claves centralizadas".
  - Envía constancia de la generación de la clave de acceso al correo del cliente.
- Afiliación a la Clave Dinámica Digital
  - Vincula el equipo celular con el cliente, para el uso de la aplicación y así pueda ser utilizado posteriormente como el único equipo autorizador.

- Afilia y Activa la Clave Dinámica con el equipo celular.
- Envía constancia de la Afiliación y Activación a la CDD al correo del cliente.

– Otras acciones de Activación

Graba BD o lista de Activaciones donde se debe almacenar DNI, Celular, Correo, Log y otros datos que se consideren necesarios. Esta BD será utilizada para el control de registro único del celular y el correo.

7.4. Afiliación a la Clave Dinámica Digital (CDD)

a Alcance

– **Afiliación a la CDD en Banca Móvil con Bio-Facial**
  - Proceso nuevo que permite al cliente afiliarse a la CDD en el canal Banca Móvil, validando su identidad con el servicio de biometría facial.
  - Considera el proceso de Migración a la CDD para clientes que cuentan con el token físico.

– **Afiliación a la CDD en Agencia + Activación en App:**
  - Inicia con la Afiliación a la CDD en ventanilla (integrada a la validación de identidad con biometría dactilar) y culmina con la Activación de CDD en el canal Banca Móvil.
  - Proceso para poder atender a aquellos clientes que no puedan afiliarse en el canal Banca Móvil debido a no poder validar su identidad con la biometría facial y para clientes que no tengan como documento el DNI.

b Flujo de Afiliación a la CDD en Banca Móvil

– **Invitación para Afiliación a la Clave Dinámica Digital**
  - Solo para clientes con tipo de documento DNI.
  - A los clientes que no se encuentren afiliados a la Clave Dinámica Digital, se les presentará una invitación para que se afilien directamente en el canal Banca Móvil.
  - El sistema verifica si el cliente se encuentra afiliado a la Clave Dinámica Digital, para lo cual debe manejar tres estados:
    ⇒ 0-No afiliado: Cliente debe ser invitado a afiliarse.
    ⇒ 1-Afiliado y pendiente de activación: Significa que el cliente se afilió en una Agencia y debe ser **invitado** a Activar su afiliación. **Proceso ya implementado**.
    ⇒ 2-Afiliado y Activado: No requiere ninguna acción.
  - Mediante Link informativo
    ⇒ Implementar un link informativo en la pantalla principal invitando al cliente a afiliarse a la Clave Dinámica Digital. "Afíliate a la Clave Dinámica Digital y realiza tus operaciones de manera segura"

⇒ El Link solo debe mostrarse cuando el cliente no se encuentra afiliado a la Clave Dinámica Digital.

⇒ Al seleccionar el link, el sistema ingresa directamente a la pantalla de Afiliación a la Clave Dinámica Digital. De lo contrario, puede acceder a la opción por la ruta del menú: Seguridad → Clave Dinámica Digital → Afiliación.

- Mediante pantalla popup

Ilustración 4: Flujo de afiliación a la CDD de la Banca Móvil (imagen referencial)

Fuente: Banca Digital – Subgerencia de Innovación Digital

⇒ Implementar en la aplicación de Banca Móvil una pantalla popup Informativa, para invitar al cliente a que se Afilie a la Clave Dinámica Digital.

- Tomar de base la pantalla existente para invitar al cliente a Activar su Clave dinámica cuando se afilia en una Agencia.
- Ajustar el mensaje informativo para indicar que la Afiliación es 100% digital.
- Eliminar el botón de Anular afiliación, ya que no existe afiliación previa y colocar en su lugar "Omitir, volver más tarde". La selección de esta opción lo lleva a la pantalla principal de saldos y movimientos.
- La opción de "Activar y vincular a Clave Dinámica Digital lleva al cliente a la pantalla de Activación.

⇒ Ejecuta la invitación de acuerdo al estado de afiliación del cliente:
- 1-Afiliado y pendiente de activación: presenta la pantalla ya existente para invitarlo a activar su clave dinámica que ya fue afiliada en ventanilla.
- 0-No afiliado: presenta la pantalla nueva propuesta para invitar al cliente a afiliarse y activar su clave dinámica desde el canal Banca Móvil.

⇒ Capacidad de configurar la frecuencia de presentación de la pantalla popup de invitación, configurando oportunidades de invitación inicial y repeticiones en el tiempo.

- **Afiliación a la Clave Dinámica Digital**
  - Para clientes que se encuentren dentro del proceso de Generación de Clave de Internet, se presentará una pantalla donde se solicitará la conformidad del cliente para afiliarse a la CDD.
    - ⇒ Este indicador solo se habilita si el cliente tiene DNI y no está afiliado a la CDD, de lo contrario debe salir deshabilitada, ya que los clientes con otro tipo de documento solo pueden afiliarse a la CDD solicitando su afiliación en una Agencia.
    - ⇒ Con la confirmación del cliente, la aplicación continúa con la Pantalla de Afiliación y Activación de la Clave Dinámica Digital
  - Para clientes que ingrese a realizar su afiliación de manera directa
    - ⇒ Acceder a la opción de Seguridad o a la opción designada por el Banco en el menú principal de la Banca Móvil o Banca por Internet del BN.
    - ⇒ Para clientes que no están afiliados al Token físico o a la CDD. la opción de Clave Dinámica Digital debe incluir al texto "¡Afíliate ahora!
    - ⇒ Seleccionar la opción de Clave Dinámica Digital y luego la opción de Afiliación.
      - Esta opción solo debe estar disponible para clientes con tipo de documento DNI.
      - Para clientes con documento diferente al DNI se debe mostrar un mensaje indicando que acuda a una agencia: "Opción no disponible, puede acercarse a una Agencia para Afiliarse a la Clave Dinámica Digital"
  - Ingreso a la pantalla de Afiliación y Activación de la Clave Dinámica Digital
    - ⇒ Solo para clientes con tipo de documento DNI.

⇒ En pantalla se muestra toda la información necesaria y condiciones para la afiliación. Tomar de base la pantalla existente y modificar la información mostrada al cliente, dejando la opción de aceptación de T&C y la integración que ya existe con el proceso de activación y vinculación del dispositivo.

- El sistema debe determinar y mostrar el dispositivo desde el cual se está realizando la operación.
- Se describe el procedimiento de validación de identidad requerido: "Para confirmar tu afiliación a la Clave Dinámica Digital, deberás validar tu identidad con Biometría Facial, de lo contrario, acércate a una Agencia".
- Se describe que, al confirmar su afiliación, solo podrá autorizar operaciones desde este dispositivo: "Al confirmar tu afiliación, únicamente podrás autorizar operaciones desde este dispositivo"

⇒ Aceptar los términos y condiciones de uso de la Clave Dinámica Digital

- Es obligatorio que se acepten los términos y condiciones de uso de la Clave Dinámica Digital. Incluir link para lectura de los T&C.
- Mostrar ventana popup de advertencia. (Funcionalidad ya implementada)

Ilustración 5: Mensaje de advertencia para la afiliación de la CDD (imagen referencial)

Fuente: Banca Digital – Subgerencia de Innovación Digital

- Al confirmar la aceptación de los T&C, se integra con el servicio de validación de identidad con biometría facial.
  - Con excepción de existir un proceso previo de validación de identidad con biometría, como el enrolamiento a la Cuenta DNI, que une tres procesos: Activación de la Cuenta DNI con Validación Bio-Facial + Generación de Clave de Internet + Afiliación a la CDD.

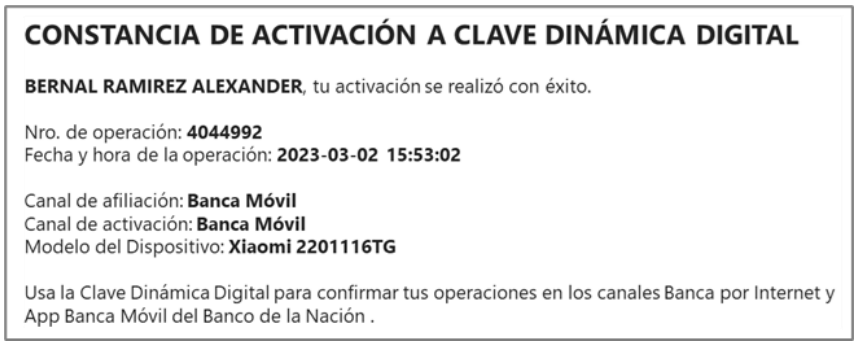
- Esta excepción solo es posible si el proceso es continuo, de lo contrario se solicita la validación de identidad de manera independiente.

- Validación de Identidad con Biometría Facial
  - ⇒ El proceso realiza la validación de identidad y retorna el resultado HIT o NO HIT.
  - ⇒ Si la validación de identidad es conforme (HIT),
    - Se ejecuta el proceso de Afiliación, Activación y vinculación del dispositivo, con lo cual queda activada la Clave Dinámica Digital.
    - Se debe registrar el código único de referencia de biometría facial para tener la trazabilidad de la validación de identidad.
  - ⇒ Si la validación de identidad no es conforme (NO HIT), se invita al cliente a la funcionalidad ya existente en Agencia mostrando un mensaje indicando "No se ha podido validar su identidad, por su Seguridad, puede acercarse a una Agencia para Afiliarse a la Clave Dinámica Digital"
- Afiliación, Activación y vinculación del dispositivo a la Clave Dinámica Digital.
  - ⇒ Proceso que Activa y vincula el dispositivo a la Clave Dinámica Digital.
  - ⇒ Se actualiza el estado de la activación de la Clave Dinámica Digital.
    - 0-No afiliado: Cliente debe ser invitado a afiliarse.
    - 1-Afiliado y pendiente de activación: Significa que el cliente se afilió en una Agencia y debe ser invitado a Activar su afiliación.
    - 2-Afiliado y Activado: No requiere ninguna acción.
  - ⇒ Se realiza la vinculación del dispositivo a la Clave Dinámica Digital. Confirmada la vinculación, únicamente podrá realizar operaciones desde este dispositivo.
  - ⇒ El canal de afiliación y activación será Banca Móvil.
  - ⇒ Registra el log de activación de CDD para poder visualizarlo en una opción del monitor de canales digitales.
- El registro de Afiliación en el sistema debe incluir la modalidad de validación de identidad utilizada y un campo para almacenar el código de referencia de la validación de identidad realizada con la biometría facial. Este campo lo retorna el servicio de biometría facial.
- Esta información deberá ser visualizada en el monitor de la aplicación en una opción de afiliaciones a la CDD.
- Se genera la Constancia de Activación de la Clave Dinámica Digital
- Mostrar en pantalla la constancia de Activación de la Clave Dinámica Digital, incluyendo la funcionalidad de compartir.

Ilustración 6: Mensaje de confirmación de la activación de la CDD (imagen referencial)

Fuente: Banca Digital – Subgerencia de Innovación Digital

- Se envía una constancia de la afiliación a la Clave Dinámica Digital al correo registrado del cliente.



CONSTANCIA DE ACTIVACIÓN A CLAVE DINÁMICA DIGITAL

BERNAL RAMIREZ ALEXANDER, tu activación se realizó con éxito.

Nro. de operación: **4044992**
Fecha y hora de la operación: **2023-03-02 15:53:02**

Canal de afiliación: **Banca Móvil**
Canal de activación: **Banca Móvil**
Modelo del Dispositivo: **Xiaomi 2201116TG**

Usa la Clave Dinámica Digital para confirmar tus operaciones en los canales Banca por Internet y App Banca Móvil del Banco de la Nación .

Ilustración 7: Constancia de activación notificada el correo electrónico del cliente (imagen referencial)

Fuente: Banca Digital – Subgerencia de Innovación Digital

c Migración a la Clave Dinámica Digital en Banca Móvil con Bio-Facial para clientes con Token físico.

- Ingresar a la opción de Seguridad en el menú principal de la APP BN.
- Seleccionar la opción de Clave Dinámica Digital y luego la opción de "Migración a CDD"

- En el menú de seguridad, al detectar que el cliente se encuentra afiliado al Token Físico, la opción de Clave Dinámica debe incluir al texto **"¡Migra ya!"**. Para clientes que no están afiliados al Token físico o a la CDD, se debe agregar el texto **"¡Afíliate ahora!"**
- Las opciones de Desafiliación y Cambio de Celular deben estar deshabilitadas o no ser mostradas, si el cliente no se encuentra afiliado a la CDD.

- Al ingresar al proceso de Migración, se debe mostrar una pantalla de advertencia indicando al cliente que se va a desafiliar del Token Físico de manera definitiva y que en adelante sólo podrá autorizar sus operaciones con la CDD.
- Si el cliente confirma la desafiliación del token físico, el sistema continúa con el "Flujo de Afiliación a la CDD en Banca Móvil"
- La confirmación de la Migración a la CDD,
  - Inicia con el flujo normal de afiliación tal como se describe en el Flujo de Afiliación descrito líneas arriba.
    - ⇒ Validación de Identidad con Biometría Facial
    - ⇒ Afiliación, Activación y vinculación del dispositivo a la Clave Dinámica Digital.
  - Validada la identidad del cliente con biometría facial y confirmada la afiliación y activación de la CDD, se procede a desafiliar al cliente del token físico.
  - Si alguna de las 2 partes de la operación fallase (la afiliación a la CDD o la desafiliación del token físico) ambas deberían revertirse.
  - Se muestra la pantalla de éxito de la migración a la CDD.
  - Se envía la constancia de migración al correo registrado del cliente y también la constancia de la desafiliación al token físico.

d Afiliación a la CDD en Agencia

- El cliente debe acercarse a una Agencia a solicitar su afiliación a la Clave Dinámica Digital y culmina en el canal Banca Móvil con la activación de la CDD:
  - Afiliación a la CDD:
    - ⇒ El Gestor de Servicios ingresa a la transacción 0280 de validación de identidad con Biometría Dactilar y valida la identidad del cliente.
    - ⇒ Luego ingresa a la transacción 4509 Afiliación a Clave Dinámica Digital y registra el número de celular del cliente y el operador de su línea. Con esto realiza la solicitud de Afiliación a la Clave Dinámica Digital y queda pendiente la activación de la misma.
    - ⇒ Registra el log de activación de CDD para poder visualizarlo en una opción del monitor de canales digitales.

⇒ Se actualiza el estado de la activación de la Clave Dinámica Digital.
- 1-Afiliado y pendiente de activación: Significa que el cliente se afilió en una Agencia y debe ser invitado a Activar su afiliación.

- Activación de la CDD:
  - ⇒ Ingresa a la App de Banca Móvil. La aplicación al detectar que el cliente se encuentra Afiliado y tiene pendiente la Activación de su Clave Dinámica Digital, lo invita en una pantalla popup, a activar su Clave Dinámica Digital: el cliente puede confirmar o desistir,
  - ⇒ Con la confirmación, la aplicación le envía una OTP al celular registrado en Agencia, el cual debe ser registrado en el sistema para validar al cliente.
  - ⇒ Si la OTP es conforme, la aplicación vincula el dispositivo celular con el Cliente, para ser utilizado como único medio de autorización para realizar las operaciones que el Banco disponga.

e Desafiliación de la CDD.

- Opción disponible en el canal Banca Móvil y Banca por Internet, seleccionar la opción de Clave Dinámica Digital y luego la opción de Desafiliación.
- Pantalla de desafiliación
  - Muestra información de la afiliación: modelo del dispositivo afiliado, fecha y celular en caso corresponda.
    - ⇒ Para las afiliaciones realizadas desde el canal Agencia, se muestra Celular, operador y modelo del dispositivo afiliado.
    - ⇒ Para las afiliaciones realizadas desde el canal Banca Móvil, solo se debe mostrar el modelo del dispositivo (no se cuenta con el dato de Celular y Operador ya que no se requiere de dicha información).
  - Solicita confirmación para desafiliar al cliente de la Clave Dinámica Digital.
    - ⇒ Actualiza el estado de la CDD a 0-No afiliado
    - ⇒ Elimina la vinculación del dispositivo móvil.
    - ⇒ Envía la constancia de la desafiliación al correo del cliente.

7.5. Gestión de Claves Centralizadas

a Objetivo

Centralizar la generación y almacenamiento de claves de acceso en una solución gestionada por el Banco a fin de optimizar el tiempo de acceso, procesamiento, control, parametrización así como incrementar la seguridad de las credenciales de los clientes (ver Anexo N° 3, Componentes Opcionales).

b Interfaces requeridas para esta funcionalidad:

i Interface para creación de la clave.
- Proceso de creación de clave: Valida identidad, registra clave en doble caja, graba clave.
- Proceso de recuperación de clave: Valida identidad, registra nueva clave, graba nueva clave.

ii Interface para cambio de la clave
- Proceso de cambio de clave: Registra clave anterior, registra clave nueva, valida clave anterior y graba clave nueva.

iii Interface para Validación de clave
- Proceso de Login: Registra clave, valida clave.
- Proceso de bloqueo: Registra Clave errada 3 veces, bloqueo automático de clave

iv Interface para bloqueo/desbloqueo
- Proceso de desbloqueo de clave: Valida identidad, solicita desbloqueo
- Proceso de bloqueo de clave: Valida identidad, solicita bloqueo.

c Descripción Funcional

i Características de la Clave
- La longitud de la Clave de Internet será de seis (06) dígitos.
- La contraseña creada por el cliente tendrá una vigencia de 365 días o un (01) año calendario.
- Parametrización de la clave de internet para los clientes por parte del Banco, esta parametrización incluye configurar la longitud de la contraseña, cantidad mínima o máxima de dígitos, caducidad de la contraseña, incorporación de caracteres y de caracteres especiales. Para este fin, el Contratista podrá proponer los mecanismos adecuados, previa autorización del Banco.
- El sistema no debe permitir contraseñas con secuencias numéricas ascendentes o descendentes, fechas de nacimiento, nombres propios (en caso de ser alfanuméricos), dígitos o caracteres repetitivos, no se empleen las tres (3) ultimas claves usadas, entre otros.
- La caducidad de la Clave de Internet debe ser notificada en la aplicación, al cliente, diariamente con diez (10) días de anticipación a su vencimiento, esta condición deberá ser parametrizable.
- Desafiliación de la clave de internet, el cliente podrá desafiliarse la clave de internet desde la Banca Móvil o también de la Banca por Internet.

ii Datos únicos para la gestión de claves
- Consideraciones:
  - Las claves deben corresponder a un Cliente (Tipo y Nro. de documento del cliente o código de cliente - CIC) y a una persona responsable autorizada para el uso de la aplicación (Tipo y Nro. de documento del responsable). Ejemplo: Una persona jurídica identificada con tipo de documento RUC y número de RUC, puede

asignar varias personas responsables autorizadas para el acceso a sus cuentas.
    - Una persona natural debe tener los mismos datos de documento como cliente y como responsable.

iii Datos clave:
- Tipo de Documento del Cliente.
- Número de documento del Cliente.
- Tipo de Documento del responsable.
- Número de documento del responsable.

iv Información requerida del módulo de gestión de claves, la cual debe ser mostrada en una consulta del módulo de gestión de claves.
- Aplicativo que invoca el servicio
- Canal que invoca el servicio
- Código del cliente (CIC)
- Tipo de documento del Cliente
- Número de documento del Cliente
- Tipo de documento del responsable
- Número de documento del responsable
- Nombre de la persona asociada al documento
- Fecha de registro de la clave
- Fecha de última actualización de la clave.
- Modalidad de validación de identidad utilizada para registrar o actualizar la clave.
    - Validación con Biometría facial
    - Validación con Tarjeta de Débito
    - Otras modalidades
- Número de operación de validación facial (parámetro enviado por la aplicación de origen, que la obtiene del servicio de validación con Bio-Facial)
- Número de la Tarjeta de Débito (dato encriptado u ofuscado, solo puede mostrar 4 últimos dígitos)
- Estado de la Clave: Activo, Bloqueado temporal, bloqueado permanente.
- Fecha y hora del cambio de estado
- Tiempo de bloqueo vigente, el desbloqueo debe colocar el dato en blanco.

v Autenticación Centralizada: Capacidad de proporcionar un único punto de autenticación que permita el acceso a los canales digitales del Banco.

vi Validación Multifactor: autenticación con dos o más factores para aumentar la seguridad.

vii Gestión de usuarios y perfiles, definidos por el Banco.

viii Control de Comportamiento del Usuario (opcional): Monitoreo y análisis del comportamiento de los usuarios para detectar actividades sospechosas o inusuales, ayudando a prevenir el fraude. El Banco decidirá hará uso de esta característica.

ix Telemetría y Análisis de Datos (opcional): Capacidad para recopilar y analizar datos sobre el uso y la interacción o el comportamiento del usuario con la plataforma, con el objetivo de mejorar la experiencia del usuario y reforzar la seguridad. Respetando la privacidad del usuario. El Banco decidirá hará uso de esta característica.

x Integración con Sistemas Existentes: El Contratista será responsable de integrar su solución con las plataformas TI que el Banco defina.

xi Cumplimiento Normativo: Cumplir con las regulaciones y normativas aplicables en materia de seguridad y protección de datos.

xii Historial de accesos: Capacidad para registrar el historial de los ingresos exitosos, intentos fallidos, tiempo de duración, equipo móvil registrado y entre otros requerimientos.

d Parámetros requeridos

i Tiempo del bloqueo temporal, por defecto 6 horas.

ii Cantidad de claves erradas consecutivas para generar el bloqueo temporal, por defecto 3.

iii Cantidad de claves históricas a validar en la generación de claves, por defecto 3 últimas.

iv Cantidad de bloqueos temporales consecutivos permitidos para generar el bloqueo permanente 3.

v Longitud de la clave, por defecto seis (06) dígitos.

vi Los puntos anteriormente mencionados deberán ser parametrizables.

7.6. Recuperación de la clave de Internet

a Consideraciones generales para la recuperación de clave de internet denominado "Olvidé mi clave de acceso" o similar:

i Se deben considerar dos escenarios para la recuperación de clave
- Clientes con Cuenta BN que tengan al menos una tarjeta.
- Clientes con Cuenta DNI, que al ser una cuenta digital no requiere información de la tarjeta.
  - Integración al servicio de biometría facial para validar la identidad del cliente.
  - La validación de identidad con biometría facial para este proceso se propone con la modalidad de "Selfie vs Mapa Facial", junto al número de tarjeta, fecha de nacimiento.

ii Se debe habilitar también la validación de identidad con biometría dactilar en agencias para aquellos clientes que no puedan identificarse con la biometría facial.

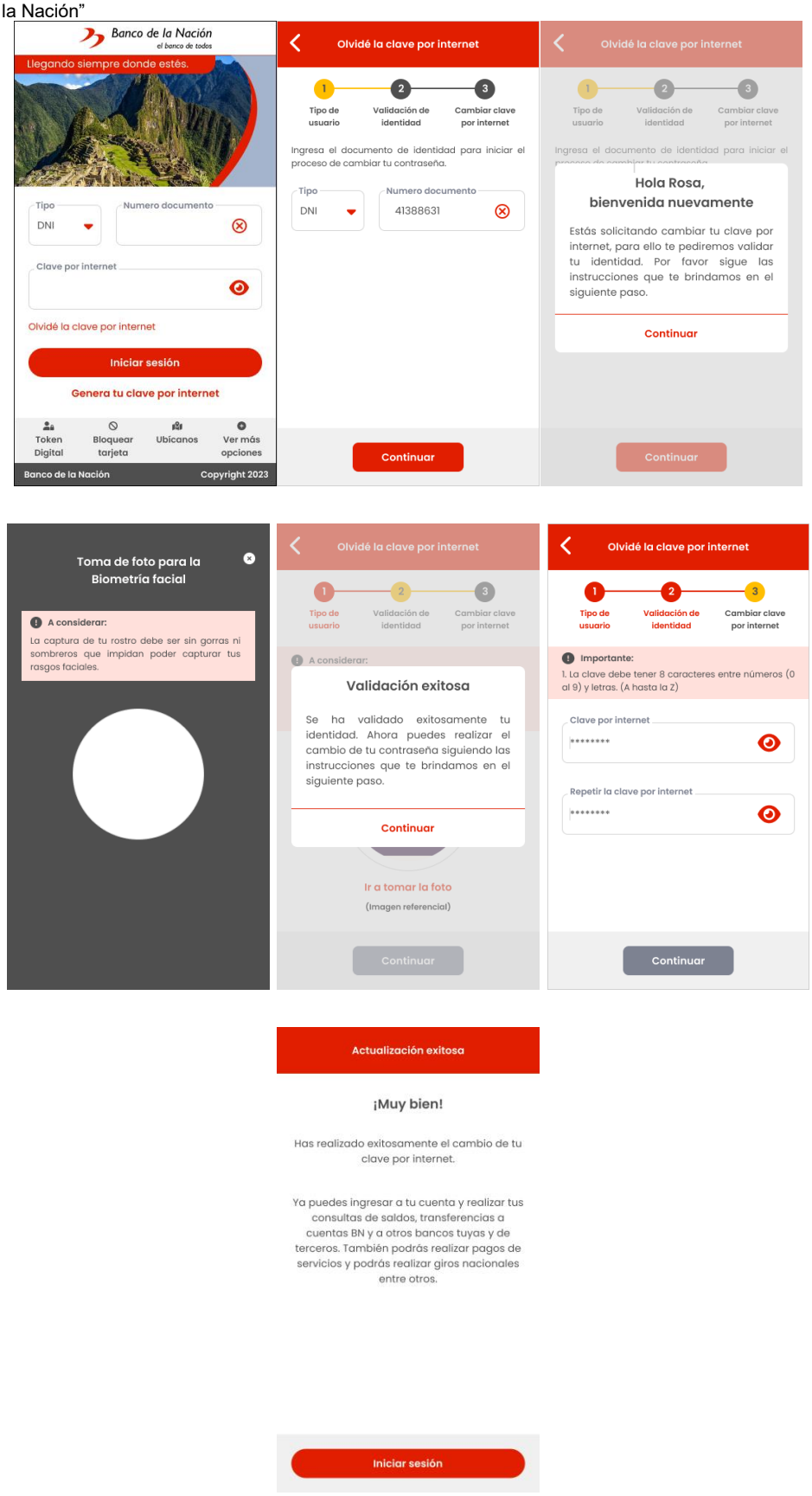


Ilustración 8: Flujo de recuperación de la clave de internet de seis (06) dígitos (Imagen referencial)

b Flujo del Proceso

i Valida cliente
- El cliente ingresa a la banca por móvil.
- Al no recordar su clave, debe ingresar a la opción "Olvidé mi Clave de Acceso" o similar.
- De acuerdo al tipo de cliente, se deriva al registro de datos de la tarjeta o se integra al servicio de biometría facial para validar la identidad del cliente.

ii Validación de Identidad del cliente con Biometría para Cuenta DNI y Cuenta BN.
- Verifica si el DNI ya tiene la bandera de validación de identidad vigente.
  - Si no tiene validación de identidad, se integra al proceso de "Validación de identidad con Biometría Facial"
  - Si tiene validación de identidad, significa que el cliente realizó su validación de identidad externa en una Agencia
    - Solicita el registro de la OTP enviada al celular del cliente cuando realizó su validación externa en ventanilla.
    - Se verifica que la OTP registrada sea válida y se encuentre vigente. Si la OTP es conforme, continúa con el proceso "Cambio de clave de acceso".
- El servicio de Bio-Facial es una caja negra que genera una respuesta de HIT o NO HIT.
  - Para este proceso se propone la modalidad de validación facial de "Selfie vs Mapa Facial", pudiendo cambiarse a criterio de las áreas competentes a otra modalidad.
  - Considerar que en este proceso ya tenemos un factor que es la posesión del dispositivo móvil seguro y la validación de identidad con biometría sería el segundo factor.
- Si la respuesta es HIT, considerando que la validación se realizó de manera integrada, continúa con el proceso "Cambio de clave de acceso"
  - Si la respuesta es NO HIT, presenta el mensaje de error en pantalla invitando al cliente para que pueda validar su identidad de manera externa en una Agencia y culmina el proceso.

iii Cambio de Clave de Acceso
- Registra la nueva clave de acceso en doble caja.
- Se debe cumplir con las restricciones del formato de la clave.
- Graba nueva clave de acceso.

7.7. Primer Inicio de Sesión

a Alcance General

La aplicación de Banca Móvil debe ofrecer a los clientes una autenticación

segura, permitiéndoles identificarse mediante su documento nacional de identidad (DNI), carné de extranjería (CE) o pasaporte en el caso de personas naturales, o utilizando el DNI del titular de la cuenta en el caso de personas jurídicas. En ambos casos, se solicitará al cliente, ya sea una persona natural o jurídica con una interfaz diferenciada, que utilice una clave de internet compuesta por seis (06) dígitos para completar el proceso de autenticación.

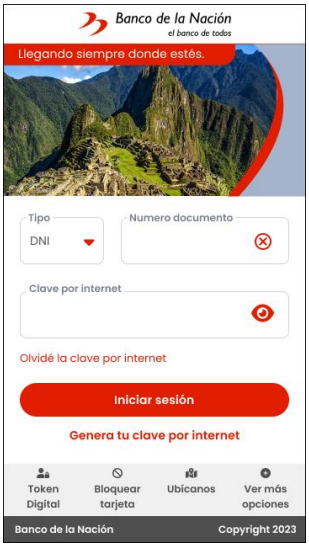


Ilustración 9: Inicio de sesión de la Banca Móvil propuesto (imagen referencial)

Fuente: Gerencia de Banca Digital

La Banca por Internet debe facilitar a los clientes la autenticación segura a través de su identificación de usuario (DNI, CE o Pasaporte) y una clave de internet compuesta por seis (06) dígitos.

Ilustración 10: pantalla de inicio de sesión al Banca por Internet del Banco de la Nación (imagen referencia)

Fuente: Informe de resultados – Servicio de experiencia de Usuario (UX/UI)

b Requerimientos Funcionales

i Precarga de la aplicación:

- La Banca Móvil y la Banca por Internet del Banco de la Nación incluirá una funcionalidad de precarga para lograr una transición fluida entre la pantalla de bienvenida y el contenido principal. La imagen de fondo del preloader será personalizable a través del Módulo de Administración de Contenidos u otro mecanismo que el Banco defina. Esta función mostrará la imagen personalizada durante un tiempo óptimo sin causar demoras significativas en la carga de la Banca Móvil y la Banca por Internet. Se adaptará a diversas condiciones de red, asegurando una experiencia consistente. Después de completar la carga, el preloader se desactivará automáticamente, garantizando una experiencia uniforme en diferentes dispositivos y sistemas operativos.

ii Identificación mediante el tipo de documento:
- La pantalla de inicio de sesión permitirá a los clientes ingresar de manera segura utilizando su número de Documento Nacional de Identidad (DNI), Carné de Extranjería o Pasaporte utilizando el teclado virtual del dispositivo registrado, asegurando una identificación precisa y confiable.
- En el campo etiquetado como "Número de documento" o similar, se implementará un cuadro de ingreso de texto que permitirá al cliente ingresar su número de DNI, Carné de Extranjería o Pasaporte utilizando el teclado virtual del dispositivo.
- La aplicación debe distinguir entre el acceso de personas naturales y jurídicas, lo cual requiere la inclusión de una opción que permita al cliente seleccionar el tipo de acceso deseado. El inicio predeterminado de la aplicación debe ser siempre en el modo de acceso de persona natural. Sin embargo, en caso de que el cliente opte por cambiar al modo de persona jurídica, este cambio debe ser visualmente distintivo para el cliente en la aplicación móvil y Banca por Internet.
  - Si el acceso es como persona natural, la aplicación le da acceso a los productos que tenga como persona natural.
  - Si el acceso es como persona jurídica, la aplicación le da acceso a los productos que tenga como persona jurídica asociadas al documento del cliente. Se deben mostrar las cuentas corrientes de persona jurídica con las funcionalidades de consulta de saldos, consulta de movimientos y descarga de estados de cuenta.

iii Clave de Internet de seis (06) dígitos:
- Los clientes deberán autenticarse mediante una clave de internet de seis (06) dígitos para garantizar un acceso seguro a sus cuentas y transacciones. Junto a este campo, se dispondrá un botón que permitirá al usuario visualizar ya que por defecto estará oculto u ofuscado los dígitos ingresados.

iv Seguridad:
- El sistema deberá garantizar la seguridad de la información transmitida o almacenada mediante medidas criptográficas o protocolos seguros de transmisión.

- En la aplicación móvil y la Banca por Internet, la entrada de los caracteres de la clave estará enmascarada u ofuscada por razones de seguridad. Sin embargo, se permitirá implementar una funcionalidad que permita al cliente visualizar los caracteres ingresados, otorgando flexibilidad al usuario.
- La aplicación móvil no deberá mostrar los caracteres ingresados a través del teclado virtual (texto predictivo) del teléfono móvil a fin de preservar la confidencialidad y seguridad de la información, esto es aplicable a todos los teléfonos celulares, indistintamente del fabricante, sin excepciones.
- Campo de Contraseña de internet: se incorporará un campo específico para que el usuario ingrese su clave de internet de seis (06) dígitos. Este campo garantizará la privacidad de la información mediante la ocultación automática de los caracteres.
  - Teclado Numérico Aleatorio: la visualización del teclado numérico para ingresar la Clave de Internet será mostrada directamente en la pantalla de manera aleatoria. Este enfoque mejora la seguridad al dificultar la identificación de patrones de ingreso.
  - Ingreso Automático: una vez que el cliente complete el ingreso del último dígito de su Clave de Internet, la aplicación móvil realizará automáticamente la validación de la información ingresada.
  - Validación de Información: en caso de que la información ingresada sea conforme y correcta, la aplicación redirigirá al cliente a la pantalla de consulta de saldos y movimientos (página de inicio) de la Banca por Internet del Banco de la Nación.

v Botón “Generar clave de internet”:
- El botón "Generar Clave de Internet" o su equivalente para nuevos clientes en el canal digital del Banco de la Nación debe ser fácilmente accesible. Al ser clic o presionarlo, deberá iniciar un proceso que guíe al cliente en la creación de su clave, verificando requisitos de seguridad y validando su identidad (consultar el enrolamiento al canal digital).
- Validar si el cliente ya cuenta con una clave generar, si no lo tiene, el cliente deberá iniciar el proceso de recuperación de clave

vi Accesos Directos en la Pantalla de Bienvenida:
- La pantalla de bienvenida de la aplicación móvil del Banco de la Nación incluirá accesos directos en la sección inferior, proporcionando enlaces rápidos a "Ubícanos", "Contáctanos" o “Bloqueo de tarjeta”. Estos accesos serán personalizables a través del Módulo de Administración (ver numeral 7.26. Módulo de Administración), brindando flexibilidad a los funcionarios responsables. Tanto clientes como usuarios podrán interactuar y acceder a información sin necesidad de iniciar sesión, asegurando un acceso sin restricciones desde la pantalla de bienvenida.

vii Cierre de Sesión:

- Al finalizar la sesión, el cliente tiene la opción de cerrar sesión para garantizar la seguridad de su información en caso de compartir el dispositivo o finalizar su actividad.
- Se debe implementar el cierre automático después de un período de inactividad de hasta tres (03) minutos, tanto para Banca Móvil como para la Banca por Internet.

c Reglas de Negocio

i Requisitos del tipo de documento:
- El DNI, CE o pasaporte proporcionado durante la autenticación debe estar registrado en el sistema del Banco de la Nación.
- El formato y la validez del número de DNI, CE o pasaporte deben cumplir con los estándares establecidos por el Banco.

ii Clave de internet:
- La clave de internet debe consistir en exactamente seis (06) dígitos.

iii Restricciones de intentos incorrectos:
- Se implementará un límite parametrizable de tres (03) intentos consecutivos fallidos de inicio de sesión con el objetivo de prevenir posibles intentos de acceso no autorizados. Una vez alcanzado este límite, se procederá a bloquear temporalmente al cliente, estableciendo un periodo parametrizable o, de manera predeterminada, por un lapso de seis (06) horas continuas.

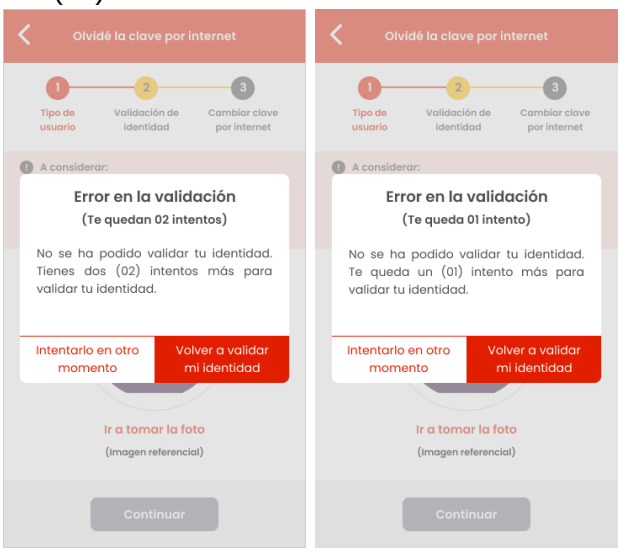


Ilustración 11: Mensajes informativos sobre los intentos disponibles para el ingreso de la clave de internet (imagen referencial)

Fuente: Gerencia de Banca Digital - Subgerencia de Innovación Digital

- Después de alcanzar este límite, se aplicará un bloqueo temporal a la cuenta y se notificará al cliente para evitar intentos de acceso no autorizados.

- En caso de que el cliente experimente tres (03) bloqueos temporales consecutivos, se procederá al bloqueo permanente de la cuenta. Se implementarán mecanismos de desbloqueo mediante biometría facial en entornos digitales o lo que el Banco considere pertinente.

iv Integración con seguridad:
- El Contratista deberá asegurar la integración con los sistemas antifraudes gestionadas por el Banco.

v Protección de Información Sensible:
- Durante el proceso de inicio de sesión, se aplicarán prácticas de encriptación para proteger la información sensible del cliente, como el número de DNI, CE, Pasaporte y la Clave de Internet.

vi Compatibilidad Dispositivos Móviles:
- La pantalla de inicio de sesión será compatible con diversos tamaños de pantalla, así como plataformas móviles y web.

vii Notificaciones de Seguridad:
- Se enviarán notificaciones de seguridad al cliente para informar sobre actividades sensibles, intentos fallidos de inicio de sesión, cambios de clave o cualquier evento relevante relacionado con la seguridad de la cuenta.

viii Caracteres numéricos
- Se restringe el uso de caracteres alfabéticos, especiales o cualquier símbolo que no sea numérico en el campo del DNI, CE o Pasaporte).

ix Proceso Onboarding para el cliente
- Para los usuarios que ingresan por primera vez, se proporcionará una orientación que destaque las ventajas de la aplicación de manera general. Esta guía abordará las necesidades que la aplicación satisface, como la reducción de ansiedad y riesgos, además de proporcionar información esencial al usuario.
- El contenido de esta sección podrá ser editable desde el Administrador de Contenidos o que el Banco defina.

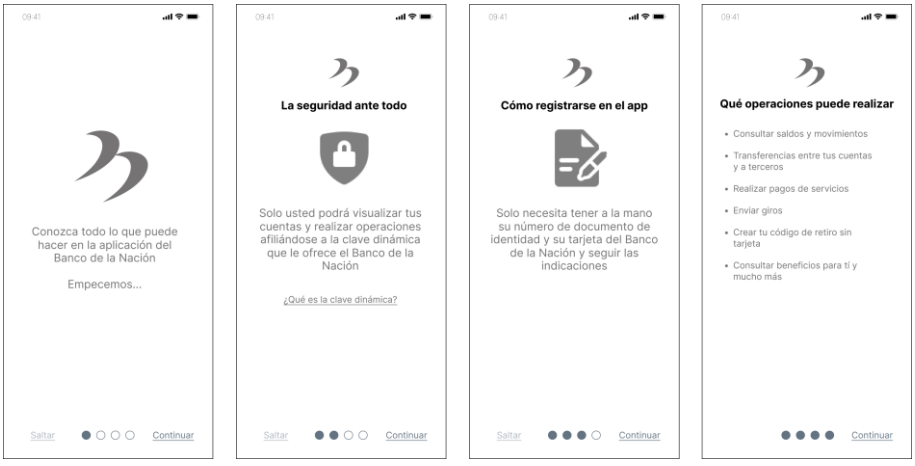


Ilustración 12: Pantallas del enrolamiento para la aplicación móvil del Banco de la Nación

Fuente: Informe de resultados – Servicio de experiencia de Usuario (UX/UI)

- d Restricciones
  - i Acceso desde dispositivos móviles Seguros:
    - El acceso a la pantalla de inicio de sesión se restringirá a dispositivos seguros (semilla de seguridad), y se desaconsejará a los clientes el uso de dispositivos modificados, en modo de desarrollado (depuración) o alterados por terceros[8] a fin de evitar posibles riesgos de seguridad.

[8] - Root (Android). Equipo editorial de IONOS. (2020, 3 febrero): acceso avanzado al sistema operativo. IONOS Digital Guide. https://www.ionos.es/digitalguide/paginas-web/desarrollo-web/root-en-android/
- Jailbreak (iOS). Equipo editorial de IONOS. (2020a, febrero 3): Romper las limitaciones del fabricante en dispositivos iOS. IONOS Digital Guide. https://www.ionos.es/digitalguide/paginas-web/desarrollo-web/jailbreak-ios/

7.8. Inicio de Sesión del Cliente Recurrente

a Alcance General

La pantalla de inicio de sesión con cliente recurrente tiene como objetivo principal ofrecer a los clientes una experiencia ágil y personalizada al acceder a la aplicación móvil y Banca por Internet del Banco de la Nación.

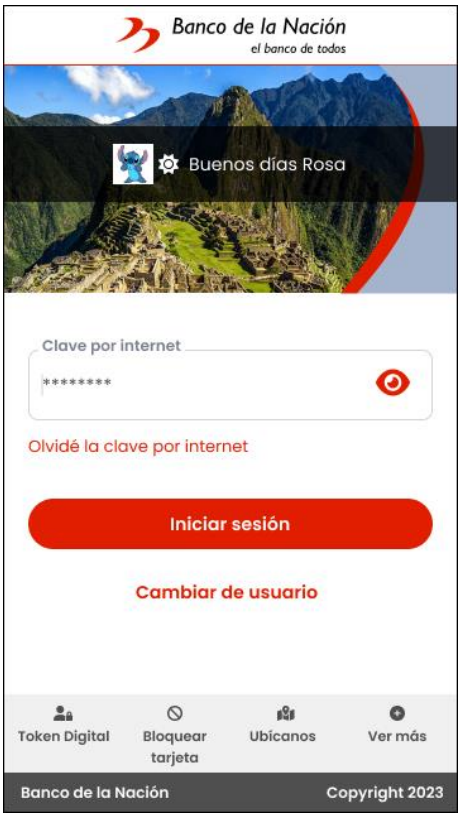


Ilustración 13: Pantalla de inicio de sesión de la aplicación móvil (imagen referencial)

Fuente: Gerencia de Banca Digital - Subgerencia de Innovación Digital

b Requerimientos Funcionales

i Identificación rápida:

- Aplicación móvil
  - El sistema deberá permitir a los clientes recurrentes ingresar sus credenciales de manera rápida y eficiente mediante la visualización automática de su nombre propio, alias o número de DNI, CE o pasaporte enmascarado u ofuscado y su clave de internet de seis (06) dígitos.
- Banca por Internet
  - El sistema deberá solicitar al usuario seleccionar el tipo de documento, ingresar el número de documento y su clave de internet de seis (06) dígitos

ii Configuración del cliente:

- Ofrece la funcionalidad de elegir el primer nombre, alias o el número de DNI enmascarado u ofuscado para clientes recurrentes, facilitando futuros accesos y mejorando la comodidad del cliente, brindándoles control sobre sus preferencias de inicio de sesión.

iii Accesos directos:

- Proporciona accesos directos a funciones clave, como comunicarse con el Banco y la ubicación de las agencias, oficinas y agentes corresponsales, mejorando la accesibilidad a servicios importantes desde la pantalla de inicio de sesión.

iv Registro de Acceso:

- Se requiere mantener un registro detallado de cada acceso (LOG), que incluya información parametrizable como la hora, ubicación, dispositivos utilizados, entre otros. Esto se realiza con el propósito de facilitar auditorías y garantizar un seguimiento efectivo de la seguridad.
- Además, se debe implementar un monitor de sucesos (LOG) que ofrezca la capacidad de visualización, así como la realización de búsquedas y filtros basados en datos principales.

v Inicio Automático al finalizar el ingreso de la Clave de Internet:

- La aplicación móvil del Banco de la Nación deberá contar con una funcionalidad que permita a los clientes iniciar sesión de manera automática al completar el ingreso del último carácter de su clave de internet. Este proceso simplificará el acceso del usuario, mejorando la experiencia de uso y agilizando el inicio de sesión en la aplicación.

c Reglas de Negocio

i Clave de internet de seis (06) dígitos:

- El número de DNI del cliente almacenado como cliente recurrente será enmascarado u ofuscado para garantizar su confidencialidad.

ii Gestión de sesión:

- Se requiere la implementación de políticas de gestión de sesiones, las cuales incluirán el cierre automático después de un período de inactividad de tres (03) minutos, con la posibilidad de ajustar este tiempo mediante parámetros configurables en el administrador.

iii Borrar cliente guardado:

- La funcionalidad permite a los clientes eliminar el nombre de usuario que tienen guardado para iniciar sesión más fácilmente. Se activa presionando el botón "x" junto al nombre de cliente en la pantalla de Login. Al presionarlo, se solicita confirmación para luego eliminar el cliente guardado. De esta forma, se mejora la seguridad y control sobre el acceso a la cuenta, obligando al cliente a ingresar sus credenciales en cada inicio de sesión en lugar de tener un cliente recordado.

d Restricciones

i Mecanismos de Autenticación Adicionales:

- Se deben implementar mecanismos de autenticación adicionales en situaciones de riesgo, como la verificación biométrica o preguntas de seguridad, para garantizar una identificación segura del cliente.

ii Escalabilidad:

- El sistema debe ser escalable para gestionar un número creciente de usuarios y transacciones, manteniendo un rendimiento óptimo en diferentes condiciones de carga.

7.9. Factores de Autenticación y Seguridad del Cliente

a Alcance General

La nueva plataforma de la Banca Móvil y la Banca por Internet deberá implementar al menos dos factores de autenticación para verificar la identidad de los usuarios durante el acceso a la plataforma bancaria. Estos factores pueden incluir algo que el usuario conozca, algo que posea y/o algo inherente a su persona, en cumplimiento de la Resolución N° 504-2021 de la Superintendencia de Banca, Seguros y AFP (SBS).

Sin perjuicio a lo anterior, se requiere que los canales digitales cuenten con la autenticación multifactorial para el proceso de enrolamiento y proceso autorización para las transacciones financieras (Clave Dinámica Digital) en los canales digitales:

b Enrolamiento al Canal Digital

Tabla 5: Cuadro de Enrolamiento al Canal Digital

		Banco de la Nación		Cuenta DNI	
1	**Enrolamiento al canal**	**APP**	**WEB**	**APP**	**WEB**
1.1	**Factores de validación**	**-**	**-**	**-**	**-**
a	**Número de tarjeta**	Sí	Sí	No aplica	No aplica
b	**Documento de identidad**	Sí	Sí	Sí	Sí
c	**Fecha de nacimiento**	Sí	Sí	Sí	Sí
d	**Biometría facial***	No aplica	No aplica	Sí	No aplica
	Selfie + RENIEC + Foto DNI	No aplica	No aplica	Sí	No aplica

c Autenticación del Cliente para la Generación de la Clave Dinámica Digital (CDD)

Se genera a demanda del cliente

Tabla 6: Cuadro de Autenticación del Cliente para la generación de la Clave Dinámica Digital (CDD)

		Banco de la Nación		Cuenta DNI	
2	**Autenticación del cliente para la Generación de la Clave Dinámica Digital**	**APP**	**WEB**	**APP**	**WEB**
2.1	**Factores de validación con token digital (Clave Dinámica Digital)**	**-**	**-**	**-**	**-**
a	**Clave de OTP**	Sí	Sí	Sí	Sí
b	**Código o ID de instalación de la aplicación móvil (único por cliente y por dispositivo)**	Sí	No aplica	Sí	No aplica
2.2	**Factores de validación con token físico**				

a	**Clave de internet**	Sí	Sí	No aplica	No aplica
b	**Código del token físico**	Sí	Sí	No aplica	No aplica

7.10. Consulta de Productos, Saldos y Movimientos

a Alcance General

La página de inicio de la aplicación móvil y a la Banca por Internet del Banco de la Nación proporcionará a los clientes una experiencia completa y personalizada, centrándose en la consulta de productos, saldos y movimientos (página de inicio). Este alcance se basa en la premisa de que cada cliente tendrá una cuenta principal vinculada a su DNI, CE o pasaporte, desde la cual podrá gestionar y acceder a diversas tarjetas, cuentas de ahorros, cuenta DNI, préstamos y cuentas contratadas con el Banco. Esto proporcionará a los usuarios una visión integral de sus productos financieros, facilitando la gestión y monitoreo de su cartera bancaria desde un único acceso.

En ese sentido, la nueva plataforma de los canales digitales del Banco de la Nación deberá presentar, tras el proceso de inicio de sesión exitoso, la relación de productos del cliente y el saldo de su cuenta principal de manera inmediata. En cuanto a los demás saldos, se visualizarán a solicitud del cliente. El Contratista deberá proponer procedimientos a fin mejora el tiempo de respuesta de las consultas y optimizar los recursos de la Nube (número de llamadas de APIs, por ejemplo). La actualización de los saldos únicamente ocurrirá si el cliente realiza transacciones durante la sesión en la aplicación móvil o la Banca por Internet. Además, los movimientos asociados a cada producto se mostrarán conforme a la solicitud expresa del cliente.

Finalmente, el acceso a la aplicación de personas jurídicas limita las funcionalidades autorizadas a la consulta de saldos, consulta de movimientos y descarga de estados de cuenta.

b Requerimientos Funcionales

i Consulta de Productos:

- Los clientes podrán visualizar de manera clara y organizada todos los productos financieros asociados a su cuenta principal. Esto incluirá cuentas de ahorros, tarjetas de crédito, cuenta DNI, préstamos, entre otros.

Vista con máscara informativa

Vista sin máscara informativa

Ilustración 14: Máscara informativa de las principales funcionalidades (imagen referencial)

Fuente: Gerencia de Banca Digital - Subgerencia de Innovación Digital

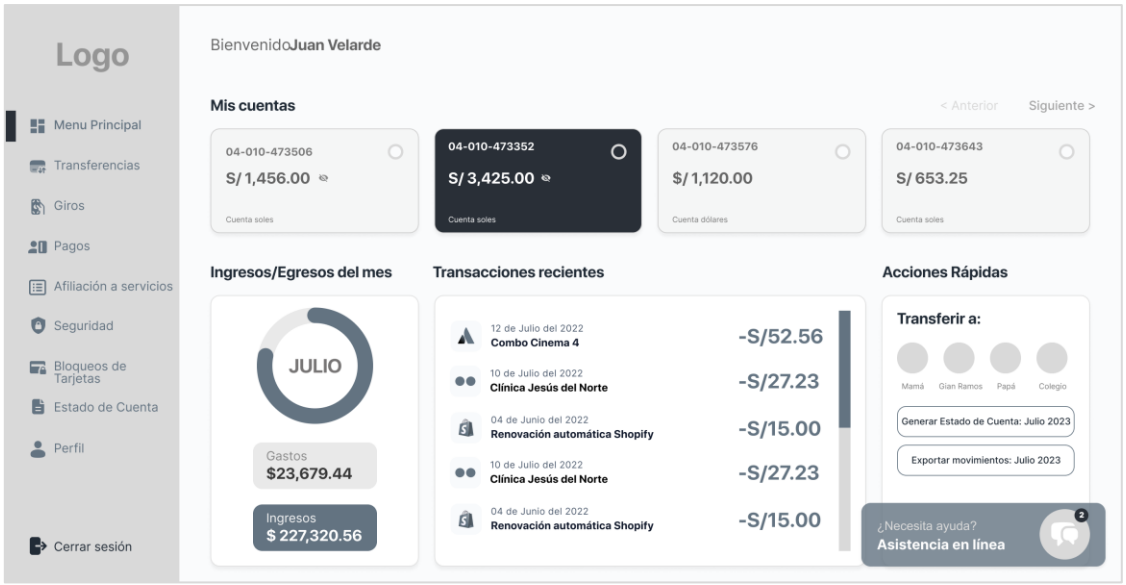


Ilustración 15: Pantalla de inicio del Banca por Internet del Banco de la Nación (imagen referencial)

Fuente: Informe de resultados – Servicio de experiencia de Usuario (UX/UI)

ii Movimientos Recientes:

- Se proporcionará un resumen de los movimientos más recientes realizados en las cuentas y tarjetas asociadas a la cuenta principal. Los clientes podrán filtrar y ordenar por criterios establecidos según los campos en pantalla.

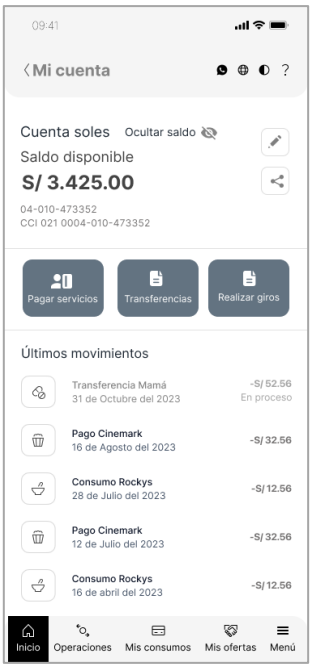


Ilustración 16: Movimientos recientes (imagen referencial)

Fuente: Informe de resultados – Servicio de experiencia de Usuario (UX/UI)

iii Accesos directos:

- La página de inicio ofrecerá accesos directos a las funciones más utilizadas, como transferencias (por contacto, por QR o por transferencia bancaria), pagos de servicios, giros, retiros sin tarjeta, retiros por agente corresponsal y consultas detalladas de movimientos. Estos accesos permitirán a los clientes realizar operaciones de manera eficiente desde el primer vistazo.

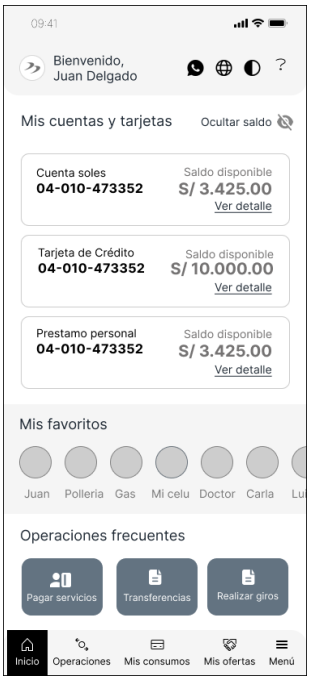


Ilustración 17: Accesos directos (imagen referencial)

Fuente: Informe de resultados – Servicio de experiencia de Usuario (UX/UI)

iv Ocultar saldos:

- Permite al cliente ocultar los saldos disponibles de sus cuentas y productos financieros en la aplicación móvil del Banco de la Nación.

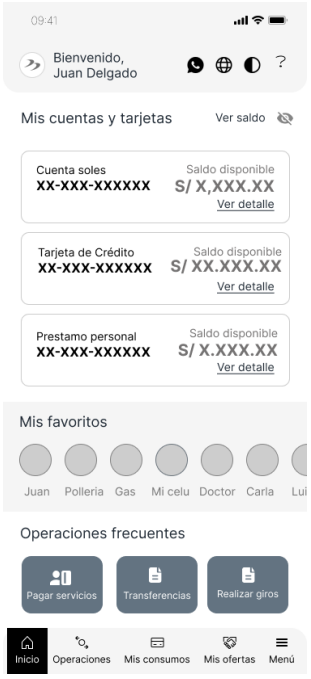


Ilustración 18: Ocultar saldos (imagen referencial)

Fuente: Informe de resultados – Servicio de experiencia de Usuario (UX/UI)

v Promociones y comunicados:
  - Muestra información importante de parte del Banco de la Nación para el cliente.

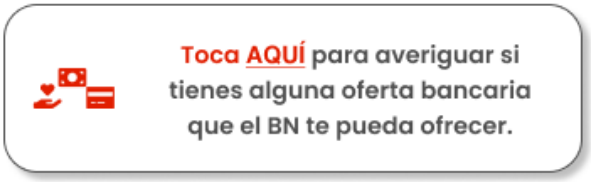


Ilustración 19: Promociones y comunicados (imagen referencial)

Fuente: Gerencia de Banca Digital - Subgerencia de Innovación Digital

  - La aplicación móvil contará con una sección de alertas y avisos ubicada en la página principal después del login, destinada a comunicar de forma proactiva al cliente situaciones relevantes asociadas a sus productos, operaciones del Banco, requerimientos de información o acciones a realizar.
  - Esta funcionalidad permitirá publicar alertas puntuales como que el cliente no cuenta aún con su Clave Dinámica Digital para realizar transacciones, necesidad de actualizar datos personales vencidos, comunicar mantenimientos programados en los canales digitales, informar cortes intermitentes del servicio, e indicar cualquier otro evento o requerimiento prioritario para la atención y conocimiento del cliente.

vi Operaciones favoritas:
  - Accesos directo para las operaciones favoritas. Al pulsar sobre cada operación, el cliente podrá visualizar el detalle de la transacción.

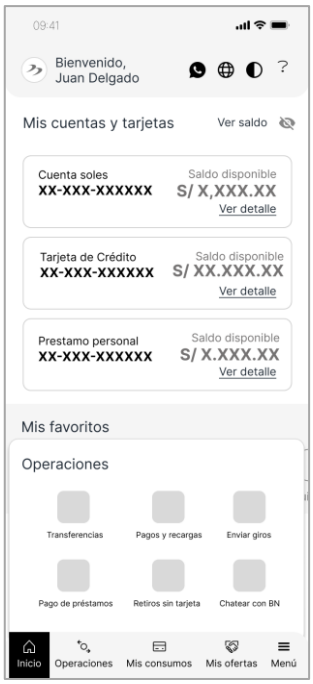


Ilustración 20: Operaciones favoritas (imagen referencial)

Fuente: Informe de resultados – Servicio de experiencia de Usuario (UX/UI)

vii Menú anclado

- El pie de página proporciona accesos rápidos a secciones adicionales, incluyendo "Inicio", "Operaciones Favoritas", "Seguridad" y "Ver Más". Al seleccionar "Ver Más", se despliegan opciones adicionales, como información de contacto para comunicarse con el Banco, términos y condiciones, políticas de privacidad, enlaces legales, cambio de idioma de la aplicación, y la opción segura para cerrar la sesión del cliente, entre otras funciones. Este diseño intuitivo facilita la navegación y el acceso a diversas funcionalidades de la aplicación.

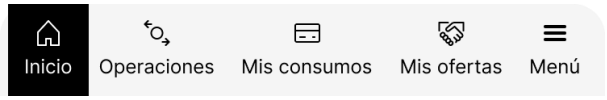


Ilustración 21: Menú Anclado (imagen referencial)

Fuente: Informe de resultados – Servicio de experiencia de Usuario (UX/UI)

7.11. Transferencias Bancarias

a Alcance General

La aplicación móvil y la Banca por Internet incorporará la funcionalidad de realizar transferencias bancarias inmediatas o diferidas, tanto a cuentas dentro del mismo Banco de la Nación como a cuentas de otros Bancos a nivel nacional, mediante cuenta bancaria, código de transferencia bancaria (CCI), cuenta corriente, número de contacto telefónico, Cuenta DNI o código QR. Asimismo, se mantendrá un historial detallado de las transacciones financieras realizadas por

el cliente.

Es preciso mencionar que, en la Banca por Internet se incluirá la transferencia por contacto, introduciendo el número de celular del beneficiario.

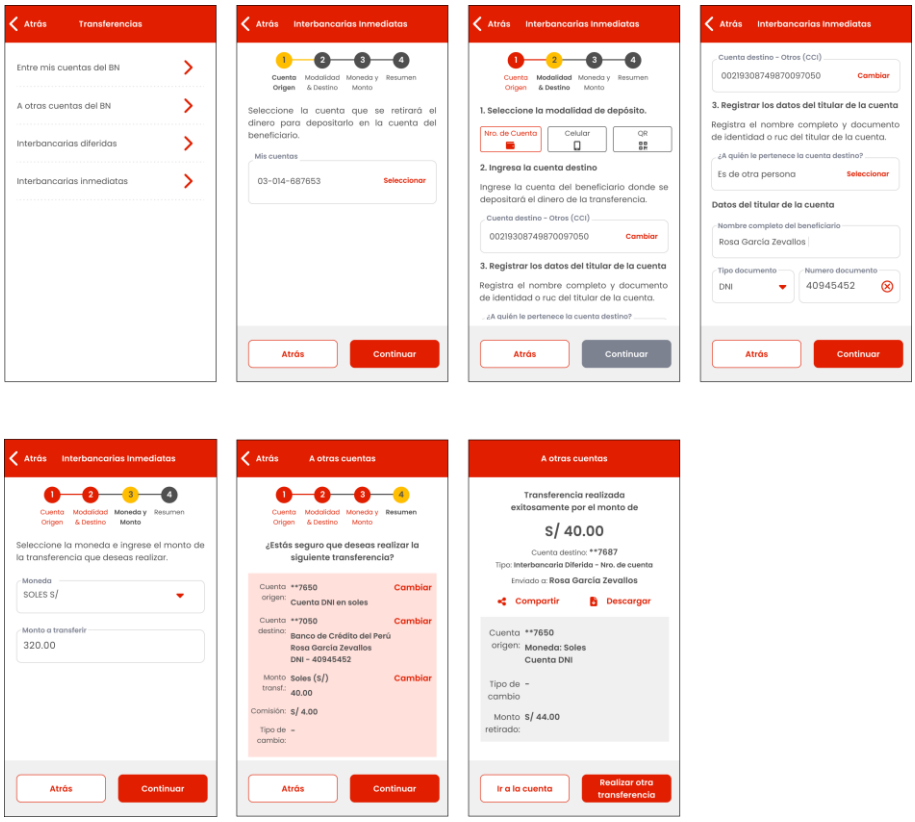


Ilustración 22: Transferencias bancarias (imagen referencial)

Fuente: Gerencia de Banca Digital - Subgerencia de Innovación Digital

b Opciones disponibles de transferencias

i Transferencias Internas:
- "Mis cuentas",
- "A cuenta BN",
- "A cuenta DNI"

ii Transferencias Interbancarias:
- "Inmediata otro Banco",
- "Diferida otro Banco"

iii Transferencias por contacto y QR

c Transferencias entre mis cuentas

i Ingresar a la opción de Transferencias y selecciona la opción "Transferencia Interna – Mis Cuentas"

ii Pantalla de Transferencia Interna
- Cuenta Origen: Permitir la selección de una cuenta de ahorros propia, disponible en la lista de productos del cliente.

- Registrar la modalidad de transferencia: la modalidad se deja seleccionada por "Nro. Cuenta" y no se permite modificar.
- Cuenta Destino: Permitir la selección de la cuenta de destino, disponible en la lista de productos del cliente.
- Registra la moneda de la transferencia: La moneda será tomada de la cuenta de destino y no se permite modificar.
- Solicitar el registro del monto a transferir
  - Validar el monto mayor a S/ 1.00 y menor o igual a S/ 2,000.00 (Considerar la parametrización por canal y transacción en el backoffice de la aplicación)
  - Construir los mensajes de alerta e informativos a mostrar respecto del monto, tomando la información de la tabla de parámetros.
  - La aplicación realiza una validación previa con sus parámetros de manera local.
  - Con los datos confirmados, se integra al servicio de consulta de transferencia interna al Core

iii Consulta de transferencia - Core Bancario
- Recibe solicitud de consulta de transferencia interna
- Ubica datos de cuenta de origen y destino considerando si son cuentas BN o Cuenta DNI.
- Cuenta de origen: Valida de manera previa las restricciones, límites y saldo de la cuenta para recibir un cargo.
- Cuenta de destino: Valida de manera previa las restricciones, límites y saldo de la cuenta Para recibir un abono.
- Determina la comisión a cobrar en caso de corresponder.
- Retorna los datos para continuar con la pantalla de confirmación de transferencia.

iv Pantalla de confirmación de transferencia
- Mostrar los datos de la transferencia
- Autorizar con la CDD.
- Solicitar confirmación de la operación.
- Con la confirmación de la operación, se integra al servicio de ejecución de la transferencia

v Ejecución de transferencia – Core bancario
- Integración con el Core a fin de ejecutar la transferencia interna.
- El Core ejecuta la operación y retorna los datos de confirmación con el número de operación.

vi Pantalla de éxito
- Se presenta la pantalla con los datos confirmados de la transferencia.
- Se habilita la opción para grabar una operación frecuente.
- Se construye la constancia de la transferencia y se envía al correo registrado del cliente.
- Se permite compartir la constancia de pantalla por los medios que dispone el sistema operativo del celular.

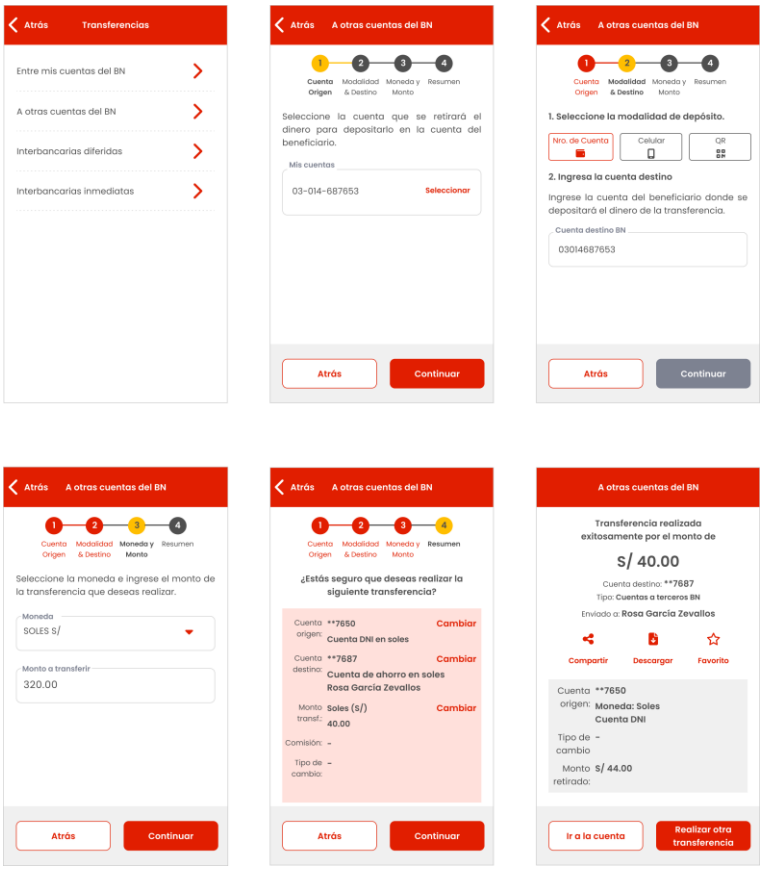


Ilustración 23: Transferencia interna (imagen referencial)

Fuente: Gerencia de Banca Digital - Subgerencia de Innovación Digital

d Transferencias a otra cuenta BN o cuenta DNI

i Ingresar a la opción de Transferencias y selecciona la opción "Transferencia Interna – Mis Cuentas"

ii Pantalla de Transferencia Interna

- Cuenta Origen: Permitir la selección de una cuenta de ahorros propia, disponible en la lista de productos del cliente. Si el cliente tiene una sola cuenta, mostrar seleccionada esa cuenta por defecto.
- Registrar la modalidad de transferencia:
  - Nro. Cuenta: requiere el registro del número de cuenta de destino.
  - Contacto: Requiere el registro del número de celular que tiene afiliado la cuenta de destino. Abre la lista de contactos para seleccionar.
  - QR: Requiere la lectura de un código QR.
- Registrar datos de la cuenta de destino o número de celular o QR
  - Transferencia con Cuenta
    - Registrar el número de cuenta (para cuenta BN) o el número del DNI (para cuenta DNI)
    - Validar la estructura del registro: implementar una rutina que permita validar ambos tipos de datos: número de cuenta de 11 dígitos y número de DNI de 8 dígitos numéricos. Para números

de 11 dígitos validar que inicie con los dos dígitos de los tipos de cuenta BN.

- Transferencia por Contacto con número de celular
  - Requiere previamente la afiliación a trasferencias por contacto integrada a un directorio interno del BN (Cuenta BN → Celular). Ver "Afiliación a Transferencias por Contacto"
  - Registrar número de celular que será validado con el directorio interno de Afiliación a contacto.
  - Integración con BD de contactos para transferencias a fin de construir lista de contactos personalizada que permita la selección de un destino.
- Transferencia por Contacto con QR
  - Abre la cámara para realizar la lectura de un código QR.
  - Genera y muestra el código QR de la cuenta de origen.
  - Con la lectura del QR se integra al directorio interno y determina la cuenta de destino.
- El directorio interno retorna los datos de la cuenta de destino y continúa con la transferencia.

- Registra la moneda de la transferencia.
- Solicitar el registro del monto a transferir
  - Validar el monto mayor a S/ 1.00 y menor o igual a S/ 2000.00 (Considerar la parametrización por canal, transacción y moneda en el backoffice de la aplicación)
  - Construir los mensajes de alerta e informativos a mostrar respecto del monto, tomando la información de la tabla de parámetros.
  - La aplicación realiza una validación previa con sus parámetros de manera local.
  - Con los datos confirmados, se integra al servicio de consulta de transferencia interna al Core

iii Consulta de transferencia - Core Bancario

- Recibe solicitud de consulta de transferencia interna
- Ubica datos de cuenta de origen y destino considerando si son cuentas BN o Cuenta DNI.
- Cuenta de origen: Valida de manera previa las restricciones, límites y saldo de la cuenta para recibir un cargo.
- Cuenta de destino: Valida de manera previa las restricciones, límites y saldo de la cuenta Para recibir un abono.
- Determina la comisión a cobrar y el ITF en caso de corresponder.
- Retorna los datos para continuar con la pantalla de confirmación de transferencia.

iv Pantalla de confirmación de transferencia

- Mostrar los datos de la transferencia: Importe, comisión, ITF, total, destino.
- Autorizar con la CDD.
- Solicitar confirmación de la operación.
- Con la confirmación de la operación, se integra al servicio de ejecución de la transferencia

v **Ejecución de transferencia – Core bancario**

- Integración con el Core a fin de ejecutar la transferencia interna.
- El Core ejecuta la operación y retorna los datos de confirmación con el número de operación.

vi **Pantalla de éxito**

- Se presenta la pantalla con los datos confirmados de la transferencia.
- Se habilita la opción para grabar una operación frecuente.
- Se construye la constancia de la transferencia y se envía al correo registrado del cliente.
- Se permite compartir la constancia de pantalla por los medios que dispone el sistema operativo del celular.

e Transferencia interbancaria inmediata

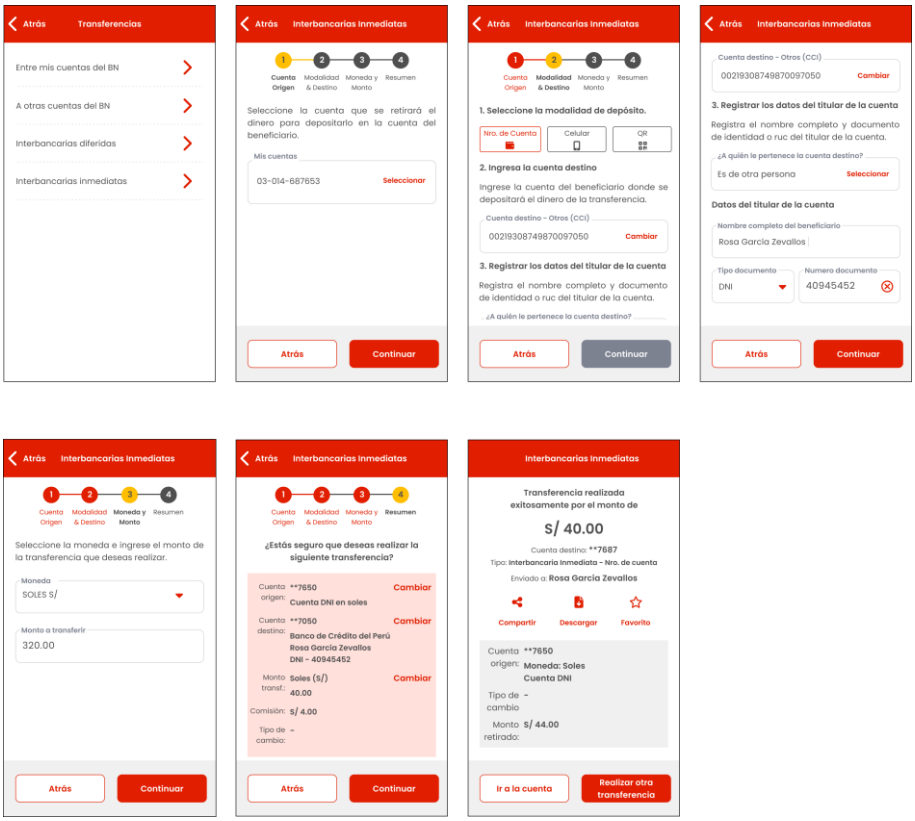


Ilustración 24: Transferencia interbancaria inmediata (imagen referencial)

Fuente Banca Digital

i **Ingresar a la opción de Transferencia y selecciona la opción** "Transferencia interbancaria inmediata"

ii **Pantalla de Transferencia Interbancaria Inmediata**

- Permitir la selección de la Cuenta de origen del cliente.
  - En caso el cliente tenga una sola cuenta, mostrar la cuenta origen por defecto.
- Mostrar tipo de modalidad de transferencia: cuenta, cuenta corriente, número de celular o código QR.
- Mostrar por defecto la moneda "Soles". Permitir el cambio de moneda a dólares.
- Mostrar la opción para que el cliente pueda ingresar una nota con un número limitado de caracteres, la aplicación permitir el ingreso solo de letras o números.
- Registrar la modalidad de transferencia:
  - Nro. CCI: requiere el registro del número de CCI de destino.
  - Contacto: Requiere el registro del número de celular que tiene afiliado la cuenta de destino. Abre la lista de contactos para seleccionar.
  - QR: Requiere la lectura de un código QR.
- Registrar datos de la cuenta de destino o número de celular o QR
  - Transferencia con CCI
    - Registrar CCI y validar la estructura del número del CCI. 20 dígitos numéricos.
  - Transferencia por Contacto con número de celular
    - Requiere previamente la afiliación a trasferencias por contacto integrada con la plataforma de interoperabilidad de la CCE, del número de celular asociado con la cuenta del cliente. Ver "Afiliación a Transferencias por Contacto"
    - Registrar número de celular que será enviado a la CCE para determinar el CCI de la cuenta de destino.
    - Capacidad para seleccionar el celular de la lista de contactos.
    - Integración con BD de contactos para transferencias para construir lista de contactos personalizada.
  - Transferencia por Contacto con QR
    - Con el QR se integra al directorio de la CCE y determina la cuenta de destino.
    - El directorio de la CCE retorna los datos de la cuenta de destino y continúa con la transferencia.
  - Solicita al orquestador BN que gestione la consulta de datos con la CCE y el Banco de Destino.
- Solicitar el registro del monto a transferir
  - Validar el monto mayor a S/ 1.00 y menor o igual a S/ 2,000.00.
  - Se integra al Core Bancario de la cuenta origen para validación de datos.

iii Flujo del Proceso

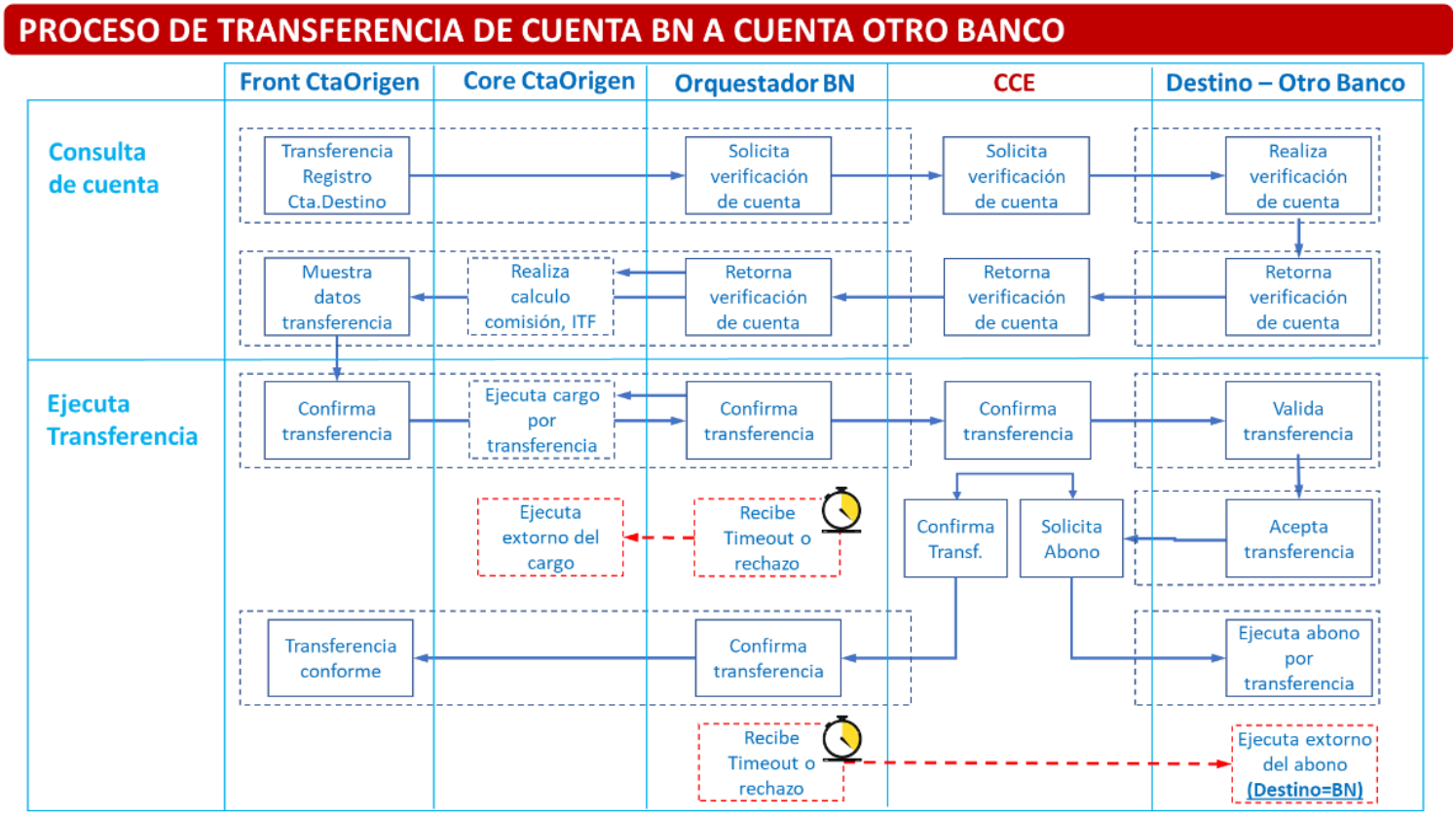


Ilustración 25: Proceso de transferencia de cuenta interbancaria

Fuente: Gerencia de Banca Digital - Subgerencia de Innovación Digital

- Front
  - Registra datos de transferencia
- BN-Orquestador
  - Gestiona consulta de datos del Banco destino con la CCE
- CCE
  - Valida cuenta de destino de manera local en su base de datos local o con el Banco de destino
    - Nombre del cliente
    - DNI del destino para determinar si coincide titularidad con el origen
  - Retorna datos al orquestador BN
- BN-Orquestador
  - Gestiona los cálculos de la transferencia con el Core de la cuenta de origen: Valida restricciones de la cuenta, Calculo del ITF, determina comisión y monto total de cargo.
  - Retorna datos al front para ser mostrados al cliente.
- Front
  - Muestra el detalle de la transferencia al cliente
  - Solicita confirmación de la transferencia con la CDD desde el único dispositivo autorizado.
- BN-Orquestador

- Recibe confirmación del front (cliente)
- Gestiona la orden de transferencia con la CCE
- Gestiona cargo en la cuenta de origen

– CCE
  - Valida reglas, registra cargo en la cuenta operativa del Banco origen en el BCRP y ejecuta la transacción de transferencia.
  - Solicita la confirmación del Banco destino para recibir el abono por la transferencia.
  - Si el Banco destino aprueba la transferencia, se realiza el abono a la cuenta operativa del Banco destino en el BCRP.
  - Con la información confirmada
    - Gestiona abono con el Banco destino
    - Confirma la transacción exitosa al Banco origen.

– Front: Pantalla de éxito
  - Se presenta la pantalla con los datos confirmados de la transferencia.
  - Se habilita la opción para grabar una operación frecuente.
  - Se envía constancia de la transferencia al correo registrado del cliente.
  - Se permite compartir la constancia de pantalla por los medios que dispone el sistema operativo del celular.

f Transferencia interbancaria diferida

La transferencia bancaria diferida estará habilitada en casos donde el servicio de transferencia inmediata no esté disponible o cuando la entidad financiera receptora no cuente con los mecanismos necesarios para recibir transferencias inmediatas desde el Banco de la Nación.

i **Ingresar a la opción de Transferencia y selecciona la opción** "Transferencia interbancaria inmediata"

ii **Pantalla de Transferencia Interbancaria Inmediata**

– Permitir la selección de la Cuenta de origen del cliente.
  - En caso el cliente tenga una sola cuenta, mostrar la cuenta origen por defecto.

– Mostrar tipo de modalidad de transferencia: cuenta, cuenta corriente, número de celular o código QR.

– Mostrar por defecto la moneda "Soles". Permitir el cambio de moneda a dólares.

– Mostrar la opción para que el cliente pueda ingresar una nota con un número limitado de caracteres, la aplicación permitir el ingreso solo de letras o números.

– Registrar la modalidad de transferencia:
  - Nro. CCI: requiere el registro del número de CCI de destino.
  - Contacto: Requiere el registro del número de celular que tiene afiliado la cuenta de destino. Abre la lista de contactos para seleccionar.

- QR: Requiere la lectura de un código QR.

- Registrar datos de la cuenta de destino o número de celular o QR
  - Transferencia con CCI
    - Registrar CCI y validar la estructura del número del CCI. 20 dígitos numéricos.
  - Transferencia por Contacto con número de celular
    - Requiere previamente la afiliación a trasferencias por contacto integrada con la plataforma de interoperabilidad de la CCE, del número de celular asociado con la cuenta del cliente. Ver "Afiliación a Transferencias por Contacto"
    - Registrar número de celular que será enviado a la CCE para determinar el CCI de la cuenta de destino.
    - Capacidad para seleccionar el celular de la lista de contactos.
    - Integración con BD de contactos para transferencias para construir lista de contactos personalizada.
  - Transferencia por Contacto con QR
    - Con el QR se integra al directorio de la CCE y determina la cuenta de destino.
    - El directorio de la CCE retorna los datos de la cuenta de destino y continúa con la transferencia.
  - Solicita al orquestador BN que gestione la consulta de datos con la CCE y el Banco de Destino.
- El sistema llevará a cabo una verificación automática para garantizar la disponibilidad del servicio de transferencia inmediata o verificar que la entidad financiera de destino esté equipada con los mecanismos necesarios para recibir transferencias inmediatas desde el Banco de la Nación. En situaciones en las que no se cumplan ambas condiciones, el sistema notificará al cliente acerca de los horarios de procesamiento de la transacción. Además, en caso de ser factible, proporcionará información detallada sobre tarifas y comisiones, permitiendo al usuario tomar decisiones informadas respecto a la realización de la transacción de manera inmediata.
- Solicitar el registro del monto a transferir
  - Validar el monto mayor a S/ 1.00 y menor o igual a S/ 2,000.00.
  - Se integra al Core Bancario de la cuenta origen para validación de datos.

iii Flujo del Proceso

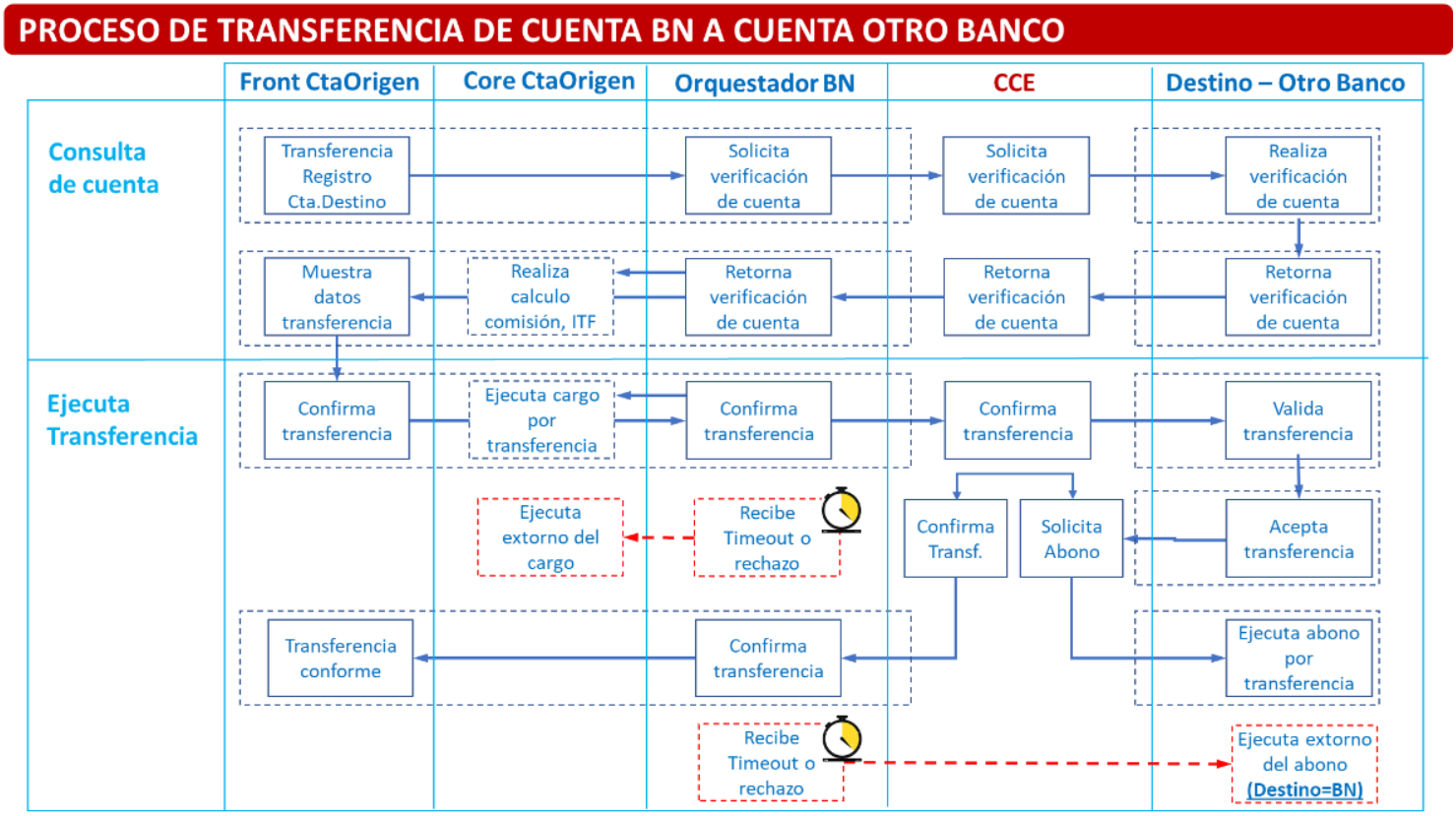


Ilustración 26: Proceso de transferencia de cuenta a otro Banco

Fuente: Gerencia de Banca Digital - Subgerencia de Innovación Digital

- Front
  - Registra datos de transferencia
- BN-Orquestador
  - Gestiona consulta de datos del Banco destino con la CCE
- CCE
  - Valida cuenta de destino de manera local en su base de datos local o con el Banco de destino
    - Nombre del cliente
    - DNI del destino para determinar si coincide titularidad con el origen
  - Retorna datos al orquestador BN
- BN-Orquestador
  - Gestiona los cálculos de la transferencia con el Core de la cuenta de origen: Valida restricciones de la cuenta, Calculo del ITF, determina comisión y monto total de cargo.
  - Retorna datos al front para ser mostrados al cliente.
- Front
  - Muestra el detalle de la transferencia al cliente
  - Solicita confirmación de la transferencia con la CDD desde el único dispositivo autorizado.
- BN-Orquestador

- Recibe confirmación del front (cliente)
- Gestiona la orden de transferencia con la CCE
- Gestiona cargo en la cuenta de origen

– CCE
  - Valida reglas, registra cargo en la cuenta operativa del Banco origen en el BCRP y ejecuta la transacción de transferencia.
  - Solicita la confirmación del Banco destino para recibir el abono por la transferencia.
  - Si el Banco destino aprueba la transferencia, se realiza el abono a la cuenta operativa del Banco destino en el BCRP.
  - Con la información confirmada
    - Gestiona abono con el Banco destino
    - Confirma la transacción exitosa al Banco origen.

– Front: Pantalla de éxito
  - Se presenta la pantalla con los datos confirmados de la transferencia.
  - Se habilita la opción para grabar una operación frecuente.
  - Se envía constancia de la transferencia al correo registrado del cliente.
  - Se permite compartir la constancia de pantalla por los medios que dispone el sistema operativo del celular.

g Afiliación a Transferencia por contacto celular

i El cliente deberá afiliar su número de celular con una cuenta de ahorros para que pueda realizar las transferencias por contacto.

ii Ingresar al menú de Transferencias y seleccionar la opción Afiliación a Transferencias por Contacto
  – Implementar tres funcionalidades
    - Afiliación: permite afiliar una Cuenta con el celular que será registrado en el directorio del Banco y/o de la CCE para las transferencias interbancarias.
    - Cambio de celular: permite cambiar el número del celular afiliado. Actualiza el número en el directorio del Banco y/o de la CCE.
    - Desafiliación: Desafilia la cuenta para realizar transferencias por contacto.

iii Selecciona la opción de Afiliación.

iv Pantalla de Confirmación para la Afiliación de Contacto para Transferencias
  – Mostrar la descripción del objetivo y el alcance de la funcionalidad
    - Objetivo: recibir transferencias con tu número de celular.
    - Alcance: Las transferencias que nos envíen pueden ser de otros Bancos o internas.
  – Implementar un Link para describir que son las transferencias por contacto.
  – Continúa con la pantalla de afiliación

v Pantalla de Afiliación
- Permite seleccionar la Cuenta a Afiliar.
  - En caso el cliente tenga una sola cuenta, mostrar la cuenta origen por defecto.
- Muestra el CCI de la Cuenta seleccionada
- Solicita el registro del celular a afiliar y debe mostrar por defecto el celular que el cliente tenga registrado.
- Seleccionar la opción de transferencia que desea registrar, se muestra seleccionada por defecto la opción completa de "Internas e Interbancarias".
  - Internas e Interbancarias
  - Solo Internas
  - Solo Interbancarias
- Continúa con la pantalla de confirmación

vi Pantalla de Confirmación
- Muestra los datos registrados para la afiliación.
- Solicita la confirmación con la CDD.
- Si confirma la afiliación, se Ejecuta la afiliación
- Integración con BN para registrar la afiliación en el directorio de afiliaciones.

vii Registra afiliación en BN
- Registra Directorio de afiliaciones para transferencia por contacto en un repositorio centralizado para uso de la Cuenta DNI y las cuentas BN.
  - Afiliación interna en un directorio interno del Banco para las transferencias de Cuenta DNI a Cuenta DNI y de Cuenta DNI a Cuenta BN o viceversa.
    - Tipo de cuenta: Cuenta BN – Cuenta BN o Cuenta BN – Cuenta DNI.
    - Número de la cuenta del cliente
    - Número del CCI de la cuenta
    - DNI del titular
    - Celular afiliado
- En caso de ser transferencia interbancaria, se integra a la CCE para registrar la afiliación en el directorio de la cámara.
  - Afiliación en el directorio de la Cámara de Compensación Electrónica para las transferencias interbancarias.
    - Tipo de cuenta: Cuenta BN – Cuenta BN o Cuenta BN – Cuenta DNI u Otros Bancos
    - Número de la cuenta del cliente
    - Número del CCI de la cuenta
    - DNI del titular
    - Celular afiliado
- El sistema debe validar que un celular solo puede estar asociado a una cuenta.
- Muestra pantalla de éxito de la operación

7.12. Retiro sin Tarjeta y por Agentes Corresponsales

a Alcance General

El requerimiento funcional tiene como propósito habilitar a los clientes de la Banca Móvil y Banca por Internet del Banco de la Nación para realizar retiros de efectivo en cajeros automáticos y agentes corresponsales sin depender de una tarjeta física. Esta funcionalidad busca ofrecer a los clientes una alternativa cómoda, conveniente y segura para acceder a efectivo.

b Requerimiento Funcional

i Ingresar a la opción Genera OTP para retiro sin tarjeta o por agentes corresponsales
- Seleccionar la Cuenta desde la cual se desea realizar el retiro.
- Mostrar el saldo disponible de la cuenta seleccionada.

ii Registrar el Monto
- Solicitar al cliente que registre el monto que desea retirar.
- Permitir que el monto pueda ser seleccionado mostrando seis cajas con montos preestablecidos que el cliente pueda elegir. Capacidad para poder configurar el valor a mostrar en cada caja.
- Si el cliente no desea seleccionar un monto preestablecido, permitir el registro directo del monto a retirar.
- Mostrar en pantalla un mensaje para el monto indicando: "Ingresa aquí la cantidad que deseas retirar (debe ser mínimo S/ 5.00 o máximo S/ 1000.00) o según lo que indique el área usuaria.
- Permitir la parametrización del rango permitido para esta operación, monto mínimo y máximo. Este mensaje debe construirse con dicha información.

iii Confirmar la generación del retiro.
- Muestra en pantalla los datos del retiro para confirmar.
- De acuerdo con el monto debe mostrar un mensaje indicando donde puede realizar su retiro:
  - Si el monto es mayor a igual a S/ 20 y es diferente de S/ 30 y es múltiplo de S/ 10
    - "Realiza tu retiro en un Agente Multired o en un Cajero Automático del Banco de la Nación"
  - Si el monto es menor a S/20 o es igual a S/ 30 o no es múltiplo de S/ 10
    - "Realiza tu retiro solo en Agente Multired del Banco de la Nación, para retiro en ATM cambie el monto a múltiplo de S/ 10, excepto S/ 10 y S/ 30"
  - Para confirmar la generación del retiro, es necesario la validación del dispositivo autorizado mediante el uso de Clave Dinámica Digital o Token Físico.

iv Genera la OTP de retiro

- Si se confirma la transacción (solo desde el dispositivo autorizado), se integra al Core bancario para la generación y envío de la OTP.
  - Actualmente la vigencia de esta OTP es de 24h registrada como parámetro y será cambiada a opinión y aprobación de las áreas involucradas. La vigencia de esta OTP se implementa en el Core.
- Si no se confirma la transacción (solo desde el dispositivo autorizado), se muestra un mensaje de error y cancela el proceso.
  - Propuesta "Su dispositivo no está autorizado a realizar esta operación, intente desde su dispositivo autorizado".

v Pantalla de confirmación de la operación

- Mostrar una pantalla de éxito de la generación del retiro.
- Mostrar un mensaje indicando "¡Ya puedes realizar el retiro de tu dinero!, Hemos enviado un código de cobro por mensaje de texto al teléfono celular *1876" o el mensaje que determine el área usuaria.
- Mostrar un segundo mensaje indicándole donde puede realizar su retiro
  - Si el monto es mayor a igual a S/ 20 y es diferente de S/ 30 y es múltiplo de S/ 10
    - "Realiza tu retiro en un Agente Multired o en un Cajero Automático del Banco de la Nación"
  - Si el monto es menor a S/20 o es igual a S/ 30 o no es múltiplo de S/ 10
    - "Realiza tu retiro solo en Agente Multired del Banco de la Nación, para retiro en ATM cambie el monto a múltiplo de S/ 10, excepto S/ 10 y S/ 30"
- Mostrar los datos del retiro: monto, fecha de la operación, número de la operación, vigencia (24h).
- Capacidad para compartir la constancia con las funcionalidades propias del sistema operativo.

7.13. Módulo de Seguridad

a Alcance General

El módulo de seguridad en aplicación móvil y la Banca por Internet del Banco de la Nación abarca la implementación de medidas y funcionalidades destinadas a garantizar la seguridad de las operaciones bancarias de los usuarios. Esto incluye la gestión de contraseñas de internet, notificaciones de actividad, generación y manejo de claves dinámicas digitales (CDD), notificaciones de actividad mediante el servicio de mensajes cortos o servicio de mensajes simples, más conocido como SMS[9] (por las siglas del inglés Short Message Service), así como características adicionales como la posibilidad de ocultar saldos o preguntas secretas por motivos de seguridad. El módulo busca

[9] Aprueban disposiciones sobre el Sistema de Notificación Electrónica de la Superintendencia de Banca, Seguros y AFP - "SISNE" - RESOLUCION - No 2291-2020 - SUPERINTENDENCIA DE BANCA, SEGUROS y ADMINISTRADORAS PRIVADAS DE FONDOS DE PENSIONES. (s. f.). https://busquedas.elperuano.pe/dispositivo/NL/1886650-1

salvaguardar la integridad y confidencialidad de la información financiera, asegurando una experiencia segura y protegida para los clientes de la aplicación móvil y Banca por Internet.

b Requerimientos Funcionales

i Cambio de clave de la contraseña de internet de seis (06) dígitos.
Proceso de cambio con verificación de clave actual y confirmación de la nueva clave, mediante el siguiente proceso:

- El cliente accede a la opción de "Cambio de Contraseña" desde la configuración de la aplicación.
- La aplicación deberá mostrar al cliente los siguientes campos:
  - Ingrese su contraseña actual
  - Ingresa tu nueva contraseña
  - Confirma tu nueva contraseña
- Se solicita al cliente ingresar su clave de internet actual de seis (06) dígitos.
  - El sistema verifica que la clave actual ingresada por el cliente sea correcta.
  - El sistema confirma el cambio mediante la CDD.
- Se muestra un mensaje de confirmación indicando que la contraseña de internet ha sido cambiada con éxito.
- Se envía una notificación al cliente sobre el cambio de contraseña a través de un mensaje en la aplicación.
- El sistema cerrará sesión en todos los dispositivos donde se abrió la aplicación.
- La aplicación redirigirá al cliente a la pantalla de inicio de sesión o login.

ii Administración de la Clave Dinámica Digital (CDD)

- La aplicación móvil del Banco de la Nación incorporará la funcionalidad de gestionar las credenciales dinámicas de un solo uso (CDD), las cuales servirán como segundo factor de autenticación de seguridad para que los clientes puedan realizar transferencias, pagos y otras operaciones bancarias.
- El cliente podrá administrar (crear o eliminar) la generación de sus propias claves dinámicas digitales sin necesidad de acudir a una agencia. Estas credenciales tendrán una vigencia temporal y será vinculada al equipo móvil fin de generar el algoritmo o semilla de seguridad.
- La aplicación mostrará en todo momento el estado actual de las CDD asociadas al cliente y permitirá obtener nuevas credenciales una vez que expiren las anteriores. Asimismo, contendrá tutoriales y guías sobre su utilización.
- La Clave Dinámica Digital (CDD) en la aplicación móvil del Banco de la Nación garantizan la generación única y vinculación al dispositivo móvil del cliente. La CDD se borra automáticamente después de cada transacción, siendo requerida especialmente para operaciones

sensibles. Se establece una actualización periódica, notificaciones al cliente sobre su generación y uso, y restricciones de uso para garantizar la seguridad y transparencia en las transacciones. Estas reglas buscan proporcionar una capa adicional de seguridad en las operaciones bancarias móviles.

viii Notificaciones de actividad por SMS o correo electrónico

- Las notificaciones electrónicas están reguladas por la Superintendencia de Banca y Seguros – SBS.
- El cliente debe registrar un número de teléfono válido o un buzón electrónico para recibir notificaciones por SMS y mensajes por correo electrónico.
- El sistema genera notificaciones por SMS y correos electrónicos para actividades como cambios de contraseña, inicio de sesión desde un nuevo dispositivo, operaciones realizadas, intentos errados de ingreso a la aplicación móvil, entre otros entre otros eventos definidos por el área usuaria.
- Los clientes no podrán desactivar la recepción de notificaciones por SMS y correo electrónico desde la aplicación móvil ni de la Banca por Internet.
- Las notificaciones por SMS y correo electrónico deben proporcionar información clara y concisa sobre la actividad realizada, evitando contenido confuso.
- Las notificaciones por SMS y correo electrónico no deben incluir información confidencial, como números de cuenta completos o contraseñas.
- El envío de notificaciones por SMS y correo electrónico debe ser consistente y oportuno, garantizando que el cliente reciba información relevante en tiempo real.

7.14. Configuración de Multidioma

a Alcance General

El objetivo de esta funcionalidad es que el Contratista implemente un mecanismo eficiente y de fácil gestión para traducir palabras o textos a diferentes idiomas. Esto se llevará a cabo a través del Administrador de Contenidos, mediante un archivo de texto plano o mediante herramientas propuestas por el Contratista, previa aprobación explícita del área usuaria.

Este requerimiento abarca el alcance de la traducción de la aplicación móvil y Banca por Internet del Banco de la Nación en quechua. Incluye la adaptación integral de la interfaz, menús, botones, etiquetas y contenido informativo al idioma seleccionado. Se busca asegurar una experiencia inclusiva y accesible para los clientes que hablan quechua. Además, se establece que la plataforma propuesta tenga la capacidad de agregar nuevos idiomas como parte de futuras mejoras a

cargo del Banco, permitiendo una expansión continua de la accesibilidad lingüística de la aplicación móvil y de la Banca por Internet del Banco de la Nación una vez que se haya implementado y puesto en producción el presente proyecto.

b Requerimientos Funcionales

i Selección de Idioma:
- Los clientes podrán seleccionar su idioma preferido desde una lista de opciones proporcionada en la aplicación, incluyendo, pero no limitado a, español o quechua como primera etapa.

ii Cambio Dinámico de Idioma:
- La aplicación permitirá al cliente seleccionar su idioma preferido, y el cambio se reflejará dinámicamente en tiempo real mediante un botón de acción disponible en la Banca Móvil y por internet.

iii Preferencias de Idioma por Cliente:
- Las preferencias de idioma se asociarán a cada usuario de manera individual, permitiendo una experiencia personalizada para cada cliente.

iv Confirmación de Cambio de Idioma:
- Se proporcionará una confirmación o mensaje de éxito una vez que el cliente haya cambiado su preferencia de idioma.

v Proceso de traducción
- Finalmente, en el proceso de traducción, los términos específicos en las lenguas originarias, como quechua y demás idiomas, se almacenarán en un repositorio. Esta base de datos permitirá una administración eficiente de los términos traducidos, facilitando su actualización y mantenimiento a través del Administrador de Contenidos, un archivo de texto plano o mediante herramientas propuestas por el Contratista, previa aprobación explícita del área usuaria. Este enfoque centralizado asegurará una coherencia y consistencia en la traducción de la aplicación móvil del Banco de la Nación, así como una capacidad ágil para incorporar nuevas traducciones y ajustes según sea necesario.

7.15. Pago de Servicios y pago a Empresas

a Alcance General

La funcionalidad de realizar pagos de servicios mediante aplicación móvil y la Banca por Internet del Banco de la Nación implica el uso de la Clave Dinámica Digital (CDD) como segundo factor de seguridad. Los clientes podrán efectuar pagos de servicios utilizando esta característica, lo que añadirá un nivel adicional de protección a las transacciones. La CDD será generada de manera dinámica y única para cada operación, asegurando la autenticación del cliente. Este proceso garantiza la seguridad en las transacciones de pago de servicios a través de la aplicación móvil, fortaleciendo la protección de la información financiera de los clientes. Asimismo, se mantendrá un historial detallado de las transacciones financieras realizadas por el cliente.

b Requerimientos Funcionales

i Selección de Servicio y Monto:
- Los clientes deben poder seleccionar el servicio que desean pagar desde una lista o directorio proporcionada por la aplicación.
- La aplicación deberá implementar un cuadro de búsqueda o filtros por tipo de servicio (cuadro de búsqueda con filtros por palabras o etiquetas).
- La aplicación deberá mostrar el monto el monto correspondiente al pago del servicio, en caso no sea posible, la aplicación permitirá al cliente ingresar el monto de forma manual.

ii Confirmación de Transacción:
- La aplicación debe mostrar los detalles de la transacción, incluyendo información del servicio y el monto a pagar.
- La aplicación debe informar al cliente que se está generando la CDD de forma automática como segundo factor de seguridad.
- La aplicación debe verificar la autenticidad de la CDD ingresada por el cliente en caso use el token físico.

iii Verificación y Autorización:
- En caso de autenticación exitosa, se autoriza la transacción y se procede al pago del servicio.

iv Confirmación y Recibo:
- Después de la autorización, la aplicación debe mostrar una confirmación de que el pago se ha realizado con éxito.
- El sistema deberá notificar al cliente de la operación realizada con los detalles de la operación.

v Registro de Transacciones:
- Todas las transacciones realizadas, incluyendo detalles del servicio y el monto, deben registrarse en la base de datos del sistema.
- El pago queda registrado en el historial con opciones de programar débitos automáticos o guardar sus pagos como favoritos, según preferencia del cliente.

vi Navegación Intuitiva:
- La interfaz de usuario debe ser intuitiva, sencilla y fácil de navegar, asegurando que los clientes comprendan claramente cada paso del proceso.

vii Seguridad de Datos:
- La aplicación debe garantizar la seguridad de los datos del cliente y de la transacción, protegiendo la información sensible durante todo el proceso.

7.16. Recargas Móviles

a Alcance General

La funcionalidad de recargas móviles de saldo en la aplicación móvil y la Banca por Internet del Banco de la Nación tiene como objetivo permitir a los clientes realizar

recargas de saldo en sus teléfonos móviles de manera rápida y segura. Asimismo, se mantendrá un historial detallado de las transacciones financieras realizadas por el cliente.

b Requerimientos Funcionales

i Operadores y Montos:
- Los clientes podrán realizar recargas para teléfonos móviles asociados a diferentes operadores de telecomunicaciones. El Banco deberá establecer los montos predefinidos y límites para las recargas.

ii Métodos de Pago:
- La aplicación admitirá diversos métodos de pago, como débito, crédito o desde la cuenta bancaria del cliente, para facilitar el proceso de recarga.

iii Confirmación de Transacción:
- Después de realizar una recarga, el cliente recibirá una confirmación inmediata en la aplicación, indicando el monto recargado y la exitosa realización de la transacción.

iv Seguridad:
- Se implementarán medidas de seguridad, como la autenticación del cliente, para prevenir transacciones no autorizadas y garantizar la integridad del proceso.

v Notificaciones:
- Los clientes recibirán notificaciones instantáneas sobre el estado de sus recargas, asegurando una comunicación efectiva y transparente.

ix Validación de Operadores:
- La aplicación verificará la validez de los operadores de telecomunicaciones asociados a los números de teléfonos móviles ingresados por los clientes antes de procesar la recarga.

x Montos Permitidos:
- Se establecerá un rango de montos permitidos para las recargas móviles, considerando límites mínimos (mayor o igual S/ 10) y máximos (menor o igual a S/ 100) a fin de garantizar transacciones seguras y acordes con las políticas del Banco. Estos parámetros deberán ser parametrizables o personalizables por el Banco, en caso de ser posible.

xi Registro de Errores:
- En caso de errores durante el proceso de pago, se registrará la información pertinente para facilitar la identificación y corrección de problemas, garantizando la transparencia y la capacidad de solucionar cualquier inconveniente.

xii Disponibilidad por Operador:
- La disponibilidad de recargas estará sujeta a la colaboración y acuerdos con los operadores de telecomunicaciones. La funcionalidad estará limitada a los operadores que participen en los convenios firmados por ambas partes.

7.17. Actualización de Datos Personales

a Alcance General

La funcionalidad de actualización de datos personales en la aplicación móvil y la Banca por Internet del Banco de la Nación tiene como objetivo permitir a los clientes realizar cambios y mantener actualizada su información personal de manera sencilla y segura.

b Requerimientos Funcionales

i Actualización para persona natural:
- Para caso de Persona Natural el cliente debe actualizar la siguiente información:
  - Nombres y apellidos completos (solo lectura).
  - Tipo de documento (solo lectura)
  - Número del documento (solo lectura)
  - Nacionalidad
  - Lugar de trabajo
  - Domicilio
  - Residencia
  - Número de teléfono
  - Correo electrónico
  - Entre otros campos definidos por el Banco

ii Restricciones en los Campos:
- Cada campo de datos personal deberá tener restricciones específicas, como el formato de correo electrónico válido, captura de datos vacíos o incompletos, la longitud adecuada para números de teléfono, y otros requisitos según la naturaleza del dato. Estas restricciones deben ser comunicadas claramente al cliente.

iii Registro de Cambios de datos personales:
- El sistema debe mantener un registro detallado de todas las actualizaciones realizadas en los datos personales. Esto incluye la fecha y hora de la modificación, el cliente que realizó el cambio y la información anterior y nueva.
- La actualización de datos personales será registrada en la Base de Datos Unificada del Cliente BDUC, propiedad del Banco de la Nación. Motivo por el cual, el Contratista deberá establecer mecanismo de comunicación (mediante APIs) con dicha base de datos a fin de asegurar el resguardo de los datos del cliente.
- El Banco podrá definir el tratamiento de los clientes persona expuesta políticamente (PEP) que no tengan información registrada.

iv Otros requerimientos de información
- El Contratista deberá implementar mecanismos parametrizables para solicitar información adicional de los clientes a través de los canales digitales, con la posibilidad de requerir información adicional en momentos posteriores al presente proyecto a fin de obtener datos relevantes.

7.18. Operaciones Favoritas

a Alcance General

La funcionalidad de registrar operaciones favoritas en la aplicación móvil y la Banca por Internet del Banco de la Nación tiene como objetivo proporcionar a los clientes una experiencia personalizada y eficiente al permitirles guardar y acceder rápidamente a aquellas transacciones que realizan con frecuencia. Las operaciones favoritas pueden incluir transferencias, pagos de servicios, recargas, entre otras.

b Requerimientos Funcionales

i Selección de Operaciones:
- Los clientes podrán seleccionar las operaciones que desean marcar como favoritas desde un menú de opciones. Este menú abarcará una variedad de transacciones favoritos, como transferencias a destinatarios habituales, pagos de servicios recurrentes y otras transacciones comunes.

ii Personalización de Nombres:
- Se permitirá a los clientes asignar nombres personalizados a sus operaciones favoritas para una identificación más rápida y sencilla. Esta personalización contribuirá a una experiencia más intuitiva y adaptada a las preferencias individuales de cada cliente.

iii Acceso Rápido desde la Página de Inicio:
- Las operaciones favoritas estarán fácilmente accesibles desde la página de inicio de la aplicación móvil. Los clientes podrán realizar estas transacciones con solo unos pocos toques, agilizando el proceso y mejorando la eficiencia en la gestión financiera.

iv Actualización de Favoritos:
- Los clientes tendrán la capacidad de gestionar y actualizar sus operaciones favoritas en cualquier momento. Podrán agregar nuevas operaciones, eliminar aquellas que ya no son relevantes o modificar los nombres personalizados según sea necesario.

v Confirmación de Transacciones:
- Al realizar una operación favorita, el sistema solicitará la confirmación del cliente antes de completar la transacción. Esto garantiza que se eviten errores y que el cliente tenga la oportunidad de revisar y autorizar cada operación.
- Al realizar una operación, el sistema mostrará un botón de acción a fin de indicar al cliente que tiene la opción de marcar como favorito la operación realizada.

vi Seguridad de la Información:
- Se implementarán medidas de seguridad robustas para proteger la información relacionada con las operaciones favoritas. Esto incluirá

métodos de autenticación y cifrado para garantizar la confidencialidad de los datos.

7.19. Giros Nacionales

a Alcance General

Facilitar a los clientes la capacidad de realizar giros nacionales de manera rápida, segura y conveniente a través de la aplicación móvil y la Banca por Internet del Banco de la Nación.

b Requerimientos Funcionales

i Inicio de Solicitud:
- Los clientes podrán iniciar el proceso de solicitud de giros nacionales desde la sección correspondiente en la aplicación móvil.

ii Selección de Monto y Destinatario:
- Los clientes podrán seleccionar el monto del giro y especificar los detalles del destinatario, incluyendo el nombre completo y el número de documento de identidad (DNI).

iii Validación de Identidad:
- El sistema verificará la identidad del cliente a través de mecanismos de seguridad, como la clave secreta (token) y, según sea necesario, la autenticación biométrica.

iv Elección del Método de Pago:
- Los clientes podrán seleccionar el método de pago para el giro, ya sea utilizando fondos disponibles en su Cuenta BN disponible para esta transacción.

v Confirmación de la Transacción:
- Antes de procesar la transacción, se proporcionará a los clientes una pantalla de resumen para revisar y confirmar los detalles del giro, incluyendo el monto, la tarifa aplicable y la información del destinatario.

vi Generación de Comprobante:
- Una vez completada la transacción, se generará un comprobante digital que el cliente podrá revisar y guardar como constancia de la operación.

vii Historial de Transacciones:
- La Banca por Internet y Banca por Internet mantendrá un historial detallado de las transacciones de giros nacionales realizadas por el cliente, accesible desde la sección correspondiente.

viii Regulaciones y Limitaciones Financieras:
- La realización de giros nacionales estará sujeta a las regulaciones y límites financieros establecidos por las autoridades bancarias y financieras. Los montos máximos y frecuencia de las transacciones podrían estar restringidos por estas normativas.

7.20. Bloqueo de Tarjeta de Débito o Crédito

a Alcance General

La funcionalidad de bloqueo de tarjeta mediante la aplicación móvil y la Banca por Internet del Banco de la Nación proporcionará a los clientes una herramienta eficiente y segura para gestionar la seguridad de sus tarjetas de crédito o débito.

b Requerimientos Funcionales

i Acceso desde la Aplicación Móvil:
- Los clientes podrán acceder a la opción de bloqueo de tarjeta directamente desde la aplicación móvil del Banco, proporcionando una interfaz intuitiva y de fácil acceso para la gestión de seguridad.

ii Selección de Tarjeta para Bloquear:
- Se permitirá a los clientes seleccionar la tarjeta específica que desean bloquear, ya sea una tarjeta de crédito o débito asociada a su cuenta.

iii Múltiples Motivos de Bloqueo:
- Los clientes podrán especificar el motivo del bloqueo de la tarjeta, como pérdida, robo o por razones de seguridad. Esta información será crucial para la gestión interna y la posterior atención al cliente.

iv Confirmación de Identidad:
- Antes de completar la solicitud de bloqueo, se implementará un proceso de confirmación de identidad del cliente para garantizar la autenticidad de la acción y prevenir bloqueos no autorizados.

v Bloqueo Inmediato:
- Una vez confirmado, el sistema procederá con el bloqueo inmediato de la tarjeta seleccionada, evitando cualquier transacción no autorizada.

vi Notificación al Cliente:
- Después de bloquear la tarjeta, el cliente recibirá una notificación instantánea a través de la aplicación móvil, brindando detalles sobre la acción realizada y los pasos a seguir.

vii Historial de Bloqueos:
- El sistema mantendrá un historial de los bloqueos realizados, proporcionando a los clientes una visión completa de las acciones de seguridad realizadas a lo largo del tiempo.

7.21. Pago de Tarjetas de Crédito

a Alcance General

La funcionalidad de pago de tarjetas de crédito a través de la aplicación móvil y la Banca por Internet del Banco de la Nación ofrece a los clientes la capacidad de realizar pagos de tarjetas tanto emitidas por el propio Banco como por otras entidades financieras.

b Requerimientos Funcionales

i Pago de Tarjetas Propias:
- Los clientes podrán realizar el pago de sus tarjetas de crédito emitidas por el Banco de la Nación de manera rápida y segura a través de la aplicación móvil. Este proceso permitirá la cancelación de saldos pendientes y la gestión eficiente de las obligaciones financieras.

ii Pago de Tarjetas de Otros Bancos:
- La aplicación permitirá a los clientes realizar pagos de tarjetas de crédito emitidas por otras entidades financieras. Se establecerán procesos seguros de verificación y confirmación para garantizar la legitimidad de estas transacciones.

iii Configuración de Cuentas para Pago:
- Los clientes podrán configurar y gestionar las cuentas desde las cuales desean realizar los pagos. Esta funcionalidad incluirá la posibilidad de asociar cuentas propias y externas para brindar flexibilidad en la fuente de los fondos.

iv Programación de Pagos:
- Se implementará la opción de programar pagos automáticos para las tarjetas de crédito, permitiendo a los clientes establecer fechas específicas para la realización automática de los pagos. Esto proporcionará comodidad y evitará posibles olvidos.

v Registro de Historial de Pagos:
- La aplicación mantendrá un registro detallado del historial de pagos realizados, ofreciendo a los clientes la posibilidad de revisar y rastrear sus transacciones de pago de tarjetas de crédito en cualquier momento.

vi Notificaciones de Pagos Exitosos:
- Los clientes recibirán notificaciones instantáneas de pagos exitosos, brindando confirmación inmediata y mejorando la experiencia del cliente al proporcionar retroalimentación en tiempo real.

vii Verificación de Pagos Externos:
- Para pagos a tarjetas de otros Bancos, se implementarán procesos de verificación adicionales para garantizar la seguridad de la transacción y prevenir posibles fraudes.

viii Pagos adelantados
- Los clientes del Banco de la Nación podrán realizar pagos adelantados[10] de sus tarjetas de crédito a través de la aplicación móvil y el Banca por Internet. El sistema permitirá ingresar el monto a pagar, seleccionar la tarjeta de crédito correspondiente y confirmar la transacción. Se aplicarán validaciones de seguridad y se proporcionará un comprobante de pago. La función estará disponible las 24 horas del día, los 7 días de la semana, a fin de brindar flexibilidad a los usuarios en la gestión de sus finanzas.

7.22. Créditos Digitales y Seguros

a Alcance General

El cliente tendrá la capacidad de solicitar, consultar y gestionar sus préstamos BN (préstamos personales, educativos, vehicular, entre otros), crédito hipotecario, seguros y asistencias, así como de tarjetas de crédito a través de la Banca Móvil y la Banca por Internet del Banco de la Nación. El sistema implementará la

[10] Superintendencia de Banca, Seguros y AFP del Perú. (s. f.). SBSPerú. Resolución S.B.S. N° 3240-2023 https://intranet2.sbs.gob.pe/dv_int_cn/2305/v1.0/Adjuntos/3240-2023.R.pdf

validación de la identidad del cliente mediante biometría facial para garantizar la seguridad del proceso, según corresponda. Asimismo, se establecerán límites máximos y mínimos para las operaciones de estos créditos digitales, con criterios validados por el Banco para asegurar la coherencia con las políticas y capacidades financieras del cliente.

b Requerimientos Funcionales:

i Solicitud de Crédito y de Seguros:
- El cliente podrá iniciar el proceso de solicitud de crédito desde la sección correspondiente en la aplicación móvil o Banca por Internet.
- Los clientes tendrán la capacidad de explorar, seleccionar y adquirir seguros optativos de acuerdo con sus necesidades y preferencias a través de la plataforma de Banca Móvil y Banca por Internet.

ii Identificación Biométrica Facial:
- La aplicación deberá contar con la capacidad de realizar una identificación biométrica facial para validar la identidad del cliente durante el proceso de solicitud, según corresponda. De acuerdo a las políticas del Banco.

iii Validación de Límites:
- El sistema verificará que el monto solicitado por el cliente se encuentre dentro de los límites establecidos por el Banco, considerando tanto límites máximos como mínimos.

iv Documentación Adicional:
- En caso de ser necesario, se indicará al cliente la documentación adicional requerida para completar la solicitud. El cliente podrá cargar dicha documentación de manera digital, de manera opcional, en caso de que Banco lo estime pertinente.

v Confirmación de Términos y Condiciones:
- Antes de enviar la solicitud, el cliente deberá confirmar su aceptación de los términos y condiciones asociados al préstamo, incluyendo tasas de interés, plazos de pago, entre otros.

vi Seguimiento de Solicitud:
- El cliente podrá realizar un seguimiento en tiempo real del estado de su solicitud, recibiendo notificaciones sobre cualquier cambio o actualización relevante.

vii Aprobación y Desembolso:
- Una vez aprobada la solicitud, el sistema gestionará el desembolso del Crédito de acuerdo con las preferencias del cliente y facilidades que cuente el Banco.

viii Histórico de Créditos:
- La aplicación mostrará un historial de los créditos solicitados y su estado actual para que el cliente pueda tener un registro completo de sus transacciones financieras.

ix Cronograma de pagos

- La aplicación mostrará el listado de la cuotas canceladas y pendientes de pago que tenga el cliente por cada uno de sus créditos.
- La aplicación mostrará el saldo deudor de cada uno de los créditos vigentes que tenga el cliente al momento de la consulta.
- La aplicación permitirá la descarga del cronograma de pagos o estado de cuenta del crédito en el tipo de formato que el Banco tenga vigente.

x Pagos de Créditos
- El cliente podrá realizar el pago de sus créditos desde su cuenta de ahorros mediante la Banca Móvil o la Banca por Internet.
- El cliente podrá realizar pagos anticipados o cancelar el total de sus créditos previa identificación y validación por los medios previamente establecidos.

xi Reglas de Negocio:
- El cliente debe ser identificado de manera segura a través de la biometría facial para poder solicitar créditos mediante la aplicación móvil y Banca por Internet.
- La validación del cliente podrá ser electrónica, esta última entendida como la que se brinda a través de un medio electrónico: ingreso de clave secreta, clave o contraseña de identificación, códigos autogenerados, haciendo clic o cliquear en dispositivos electrónicos, aceptación por voz, firma o certificado digital, medios biométricos, entre otros, que el Banco tenga a disposición.
- Las operaciones que realice el cliente por la Banca Móvil y la Banca por Internet contarán con un servicio de notificación para informar al cliente por el medio de comunicación (SMS o correo electrónico) que elija.
- El sistema debe cumplir con las regulaciones de seguridad vigentes para proteger la privacidad y confidencialidad de la información del cliente durante todo el proceso de atención del crédito.
- Se proporcionará retroalimentación clara al cliente sobre la aprobación o rechazo de la solicitud de crédito, junto con los términos y condiciones aplicables.
- El proceso de solicitud de crédito debe ser intuitivo y fácil de entender para mejorar la experiencia del usuario y permitirá afiliar servicios adicionales al crédito como seguros, asistencia y otros adicionales.

xii Restricciones
- La implementación de la biometría facial estará sujeta a la disponibilidad y compatibilidad de los dispositivos móviles y sistemas operativos utilizados por los clientes.
- Los límites máximos y mínimos para los créditos estarán determinados por las políticas internas del Banco de la Nación, y cualquier solicitud que exceda estos límites será rechazada automáticamente.
- La disponibilidad de la opción de solicitud de créditos estará sujeta a la elegibilidad del cliente, la cual será evaluada por el Banco en función de factores como historial crediticio y capacidad financiera.

- La validación de la identidad mediante biometría facial estará sujeta a la precisión y confiabilidad de la tecnología utilizada, y cualquier error en la verificación podría resultar en el rechazo de la solicitud.

7.23. Consulta de Estado de Cuenta

a Alcance General

Este alcance asegura que los clientes del Banco de la Nación puedan acceder fácilmente a su información financiera pasada, promoviendo la transparencia y el control sobre sus cuentas a través de la aplicación móvil y la Banca por Internet.

b Requerimientos Funcionales

i Visualización de Estados de Cuenta:
- Los clientes podrán consultar sus estados de cuenta de hasta seis (06) meses calendarios anteriores directamente desde la aplicación móvil.

ii Acceso Seguro:
- La consulta del estado de cuenta estará protegida por medidas de seguridad robustas, asegurando que solo los usuarios autorizados tengan acceso a información financiera sensible.

iii Histórico de Transacciones:
- Además de los saldos actuales, los usuarios podrán revisar un historial detallado de transacciones realizadas en sus cuentas durante el período especificado.

iv Filtrado por Cuenta:
- En el caso de clientes con múltiples cuentas, la aplicación permitirá la selección de una cuenta específica para consultar su estado de cuenta asociado.

v Fecha de Corte Ajustable:
- La fecha de corte para la consulta del estado de cuenta será ajustable, permitiendo a los usuarios seleccionar el período exacto que desean revisar.

vi Descarga de Estado de Cuenta:
- Se proporcionará la opción de descargar el estado de cuenta en formato digital tipo PDF con contraseña que será el número de documento (DNI, Carné de Extranjería o Pasaporte) del titular, facilitando la gestión y almacenamiento de documentos financieros.

vii Envío del estado cuenta por correo electrónico:
- Los clientes podrán activar en envío del estado de cuenta por correo electrónico, siempre y cuando, el Banco cuente con la dirección de buzón de correo electrónico.

viii Restricciones de Privacidad:
- La aplicación garantizará la privacidad de la información financiera del cliente, implementando medidas para prevenir el acceso no autorizado.

ix Cumplimiento Normativo:

- La funcionalidad de consulta del estado de cuenta cumplirá con las regulaciones financieras y de privacidad aplicables en el entorno bancario.

7.24. Ubicación de Agencias, Cajeros y Agentes

a Alcance General

La funcionalidad de consulta de ubicación en la aplicación móvil y la Banca por Internet del Banco de la Nación proporcionará a los clientes información detallada y en tiempo real sobre la ubicación de agencias, cajeros automáticos y agentes del Banco.

El proveedor gestionará las cuentas del servicio de mapas y posteriormente será trasladado al Banco. En el caso se incurra en algún costo por este servicio, este será facturado mensualmente al Banco bajo a demanda detallando el consumo realizado.

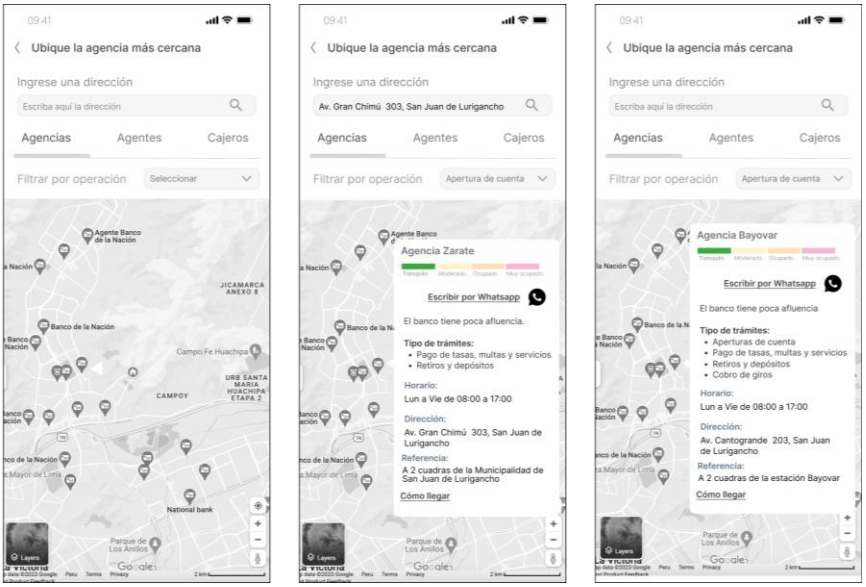


Ilustración 27: Ubicación de agencias, cajeros y agentes (imagen referencial)

Fuente: Informe de resultados – Servicio de experiencia de Usuario (UX/UI)

b Requerimientos Funcionales

i Agencias:
- Visualización de la ubicación precisa de todas las agencias del Banco de la Nación en el territorio nacional.
- Información sobre el tipo de operaciones disponibles en cada agencia.
- Horarios de atención, incluyendo días laborables y fines de semana.

ii Cajeros Automáticos:
- Identificación de la ubicación de los cajeros automáticos del Banco.
- Disponibilidad operativa en tiempo real.
- Tipo de transacciones que se pueden realizar en cada cajero.

iii Agentes del Banco:

- Localización de agentes autorizados para realizar transacciones bancarias.
- Información sobre los servicios que ofrecen.
- Horarios de atención definidos por los agentes y días de servicio.

iv Información en Tiempo Real:
- El proveedor deberá desarrollar las APIs que seán necesarias para que pueda obtener la información de las oficinas, cajeros y agentes que será proporcionado por el Banco. Se aclara la información en tiempo real se refiere a la geolocalización del equipo móvil.

v Distancia y Rutas:
- Cálculo de la distancia desde la ubicación actual del cliente hasta la agencia, cajero o agente seleccionado.
- Proporcionar rutas detalladas para llegar al destino deseado con o sin conexión al GPS[11].

vi Funcionalidad de Mapa Interactivo:
- Integración de un mapa interactivo que permita a los clientes explorar fácilmente las ubicaciones.
- Iconografía clara para diferenciar entre agencias, cajeros y agentes.

vii Filtros de Búsqueda:
- Opciones de filtro para personalizar la búsqueda según las necesidades del cliente, como tipos específicos de operaciones, UBIGEO, etiquetas o horarios de atención extendidos.

viii Acceso a la Información sin Iniciar Sesión:
- La funcionalidad estará disponible incluso para clientes que no han iniciado sesión, permitiendo un acceso rápido y fácil.

7.25. Configuración de los Atributos de Cuentas y Tarjetas del cliente

a Alcance General

Este documento establece el alcance y los objetivos de la configuración de atributos específicos de cuentas y tarjetas dentro de la aplicación móvil y la Banca por Internet del Banco de la Nación. La finalidad principal es proporcionar a los clientes un mayor control sobre ciertos aspectos clave de sus cuentas y tarjetas para adaptar su experiencia bancaria de manera personalizada.

b Requerimientos Funcionales

i Transferencias:
- Posibilidad de habilitar o deshabilitar la opción de realizar transferencias sin necesidad de tarjeta en cajeros automáticos y agentes del Banco de la Nación.

ii Giros y Retiros Sin Tarjeta:

[11] Sistema de Posicionamiento Global - GPS (s. f.). https://www.gps.gov/spanish.php

- Posibilidad de habilitar o deshabilitar la opción de realizar giros y retiros de efectivo sin necesidad de tarjeta en cajeros automáticos y agentes del Banco de la Nación.

iii Compras por Internet:
- Posibilidad de activar o desactivar la capacidad de realizar compras por internet con tarjetas vinculadas, permitiendo a los clientes controlar la seguridad de sus transacciones en línea.

iv Operaciones en el Extranjero:
- Posibilidad de activar o desactivar la capacidad de realizar operaciones con tarjetas en el extranjero, brindando a los clientes control sobre el uso internacional de sus tarjetas.

v Notificaciones por Operación:
- Envío automático de las notificaciones para recibir alertas inmediatas sobre transacciones específicas por SMS y correo electrónico, asegurando una monitorización en tiempo real de la actividad de la cuenta. Para atender el presente requerimiento, es necesario que el cliente cuente con un número celular y un correo electrónico validado.

vi Límites por transacción
- Configuración de los límites para transferencias entre cuentas propias y cuentas de terceros, proporcionando a los clientes control sobre sus transacciones.

7.26. Módulo de Administración (backoffice)

a Alcance General

El módulo de administración (backoffice) del Banco de la Nación debe permitir que el personal autorizado del Banco administre los contenidos de la aplicación sin la capacidad de consultar ni modificar saldos o realizar transacciones bancarias en las cuentas de los clientes. Esto incluye la gestión y actualización de información institucional y promocional, mensajes de seguridad, ofertas, fondos de la aplicación, notificaciones, bloqueo/desbloqueo de dispositivos y establecimiento de límites de movimientos para los clientes. Además, se debe considerar la traducción de etiquetas a otros idiomas para garantizar una experiencia completa para los usuarios de diferentes lenguas nativas del Perú.

b Requerimientos Funcionales

i Personalización del fondo de la aplicación.
- Opción de poder actualizar el fondo del inicio de sesión de las plataformas Banca por Internet y Banca Móvil.

ii Bloqueo y desbloqueo de dispositivos.
- Se podrán bloquear y desbloquear equipos determinados de usuarios seleccionados. De esta manera se podrá imposibilitar el acceso a la plataforma. Carga masiva de usuarios por DNI.

iii Roles de usuarios en el CMS

- Se podrán crear usuarios para acceder al CMS, los cuales tendrán accesos predefinidos.

iv Banners, mensajes institucionales, campañas y ofertas
- Se podrán cargar mensajes e imágenes además de un link de redireccionamiento si es necesario. La información se cargará desde un formulario predefinido.
- Envío de Notificaciones Push.
- Se enviarán de manera automática notificaciones a los usuarios al momento de crear ofertas, productos o mensajes institucionales.
- Se podrán crear ofertas para enfocadas a una lista de clientes cargada desde el CMS.
- Las ofertas contendrán banner, texto y botón de acción que consultará el servicio.

v Reportes:
- Reporte de Ofertas, muestra cantidad de interacciones, vistas, dispositivos
- Productos de productos, muestra cantidad de interacciones, vistas, dispositivos
- Usuarios conectados, Cantidad de usuarios que se encuentran utilizando la plataforma.
- Equipos, muestra el tipo de equipos que transaccionan con la plataforma.

vi Módulo de bloqueo por soporte y mantenimiento App y Web:
- Será un mensaje auto administrable desde el back office, el cual se utilizará en momentos en los cuales se vaya a realizar algún mantenimiento o actualización de la plataforma y no se contará con el servicio disponible.
- Los de usuarios: Registro de acciones realizadas en la plataforma por usuarios.

vii Mensajes de Error, de advertencia, de éxito y otros
- Por medio del back office se podrán editar los mensajes de error que se muestran a los usuarios finales de las distintas transacciones disponibles. Para esto se tomará el código de error del API y se le colocará un texto el cual podrá ser editable.

viii Guías para el usuario
- Al lanzar una nueva versión del aplicativo móvil o Banca por Internet se deberán realizar elaborar las guías de usuario o tutoriales recorridos guiados, sugerencias en pantalla al cargar la aplicación o guías de usuario. El Contratista deberá brindar los mecanismos adecuados para dicho fin cuidado el rendimiento del aplicativo móvil o Banca por Internet.

ix Administración de la sección Canales de Atención "Ubícanos"
- Mediante el módulo de administrador se actualizará los datos correspondientes a las ubicaciones: agencias, cajeros automáticos, agentes y en otras entidades financieras.

- Configuraciones parametrizables
  - Umbrales de Transacciones:
    - Montos máximos y mínimos para transferencias, pagos, depósitos y otras operaciones.
    - Límites diarios, semanales y mensuales para las diferentes transacciones.
    - Permitir o no la realización de transacciones sin autorización adicional para montos menores a un cierto valor.
  - Parámetros de Seguridad:
    - Configuración de los niveles de seguridad para las diferentes operaciones, como autenticación biométrica o doble factor.
    - Configuración de la caducidad de las contraseñas de internet para que los usuarios deban renovarlas dentro de los plazos establecidos.
    - Ajuste de la Temporalidad de la Sesión por Inactividad y en la cantidad permitida de intentos de contraseña errónea para bloquear cuentas.
  - Otros Parámetros:
    - Personalización de la interfaz de usuario como el idioma por omisión, imágenes de preloader, colores de la aplicación, actualización de iconos.
    - Permitir o no la visualización de ciertas funcionalidades a los usuarios previa autorización del Banco.
    - Habilitar o deshabilitar diferentes opciones de la plataforma propuesta, previa autorización del Banco.

7.27. Pago de Tasas

a Alcance General

La aplicación móvil del Banco de la Nación debe enlazar con la plataforma de Págalo.pe para permitir que los clientes realicen el pago de tasas e impuestos de manera conveniente. Esta integración facilitará a los clientes el cumplimiento de sus obligaciones tributarias directamente desde la aplicación móvil y la Banca por Internet.

Si el enlace no encuentra en la lista de aplicaciones disponibles en el teléfono del cliente, la aplicación deberá redirigir a la tienda de aplicaciones según corresponda a la marca del equipo móvil del cliente.

7.28. Cuenta DNI

Los Requerimientos Funcionales de la Cuenta DNI se integrarán en la nueva aplicación móvil y en la Banca por Internet del Banco de la Nación. Este proceso se llevará a cabo de acuerdo con las necesidades del Banco (ver Anexo N° 4, Cuenta DNI), las cuales serán comunicadas oportunamente al Contratista con al menos 90

días calendarios de anticipación antes de finalizar el , según el cronograma establecido.

A continuación, se presentan los requerimientos principales:

i Registro y Autenticación:
- Proceso de registro sencillo para los usuarios.
- Mecanismos robustos de autenticación, incluyendo opciones biométricas como huella dactilar y reconocimiento facial.

ii Consulta de Saldo y Movimientos:
- Acceso en tiempo real al saldo de la cuenta asociada.
- Historial detallado de transacciones y movimientos.

iii Transferencias y Pagos:
- Posibilidad de realizar transferencias entre cuentas del mismo Banco.
- Pagos de servicios básicos y otros beneficiarios registrados.
- Retiro sin tarjeta
- Retiro por agente corresponsal

iv Seguridad y Privacidad:
- Implementación de medidas de seguridad avanzadas para proteger la información del usuario.
- Respeto absoluto a la privacidad y confidencialidad de los datos.

v Notificaciones y Alertas:
- Sistema de notificaciones en tiempo real para transacciones y eventos relevantes.
- Alertas de seguridad y actividad sospechosa.

vi Integración con Otros Servicios Bancarios:
- Posibilidad de vincular y gestionar otros productos financieros ofrecidos por el Banco de la Nación y banca comercial o privada.

vii Compatibilidad con Dispositivos:
- Disponibilidad para dispositivos móviles con sistemas operativos Android y iOS.

viii Actualizaciones y Mejoras Continuas:
- Implementación de actualizaciones y mejoras de manera regular para garantizar una experiencia óptima.

ix Cancelación de la Cuenta DNI
- Finalmente, el cliente podrá cancelar su Cuenta DNI cuando lo requiera mediante el sistema.

8. ESPECIFICACIONES TÉCNICAS DEL DESARROLLO

Para el desarrollo de los nuevos canales digitales del Banco de la Nación se considerarán las últimas versiones de las tecnologías, salvo el Banco requiera alguna en versión en particular siendo estas:

Para el aplicativo Banca Móvil versión iOS:

- Lenguaje de programación Swift 5.9.2 o superior. Opcionalmente, podrá incluir otras herramientas de desarrollo.

Para el desarrollo de la Banca Móvil Android:

- Lenguaje de programación Kotlin 1.9.22 o superior. Opcionalmente, podrá incluir otras herramientas de desarrollo.

Para la banca Web y back Office:

- Lenguaje de programación Angular 17.0.7 o superior; o C# sobre la plataforma .NET Core 8 o superior.

Para el backend:

- Lenguaje de programación Java 8 o superior; o C# sobre la plataforma .NET Core 8 o superior.
- Marco de trabajo Springboot 3.2 o superior. Opcionalmente, podrá incluir otros marcos de trabajo, aprobados por el Banco.
- Cobol versión 3 o superior.

Para la Base de datos

- Servicio de base de datos SQL (basado en PostgreSQL 16.1 o similar)
- Servicio de base de datos de documentos (basado en Mongo DB 6.0.7 o similar)

9. REQUERIMIENTOS DE LA ARQUITECTURA TECNOLÓGICA

9.1. Componentes On-Premise y en la Nube

El Banco de la Nación opera su Core Bancario sobre una plataforma Mainframe IBM zSeries – Modelo Z15 con sistema operativo z/OS 2.24 (ambientes no productivos) y 2.2 (ambiente productivo). El ambiente productivo opera en el Centro de Datos de San Borja y en contingencia en el Centro de San Isidro.

Se cuenta además con una infraestructura on premise de API Gateway (IBM Cloud Pack for Integration) sobre OpenShift que se conecta a los procesos del Core Bancario a través de Microservicios en plataforma de contenedores Kubernetes.

El gráfico a continuación muestra la interacción que se propone para que la Nueva App y Web BN interactúe con los servicios del Core Bancario On-Premise del BN.

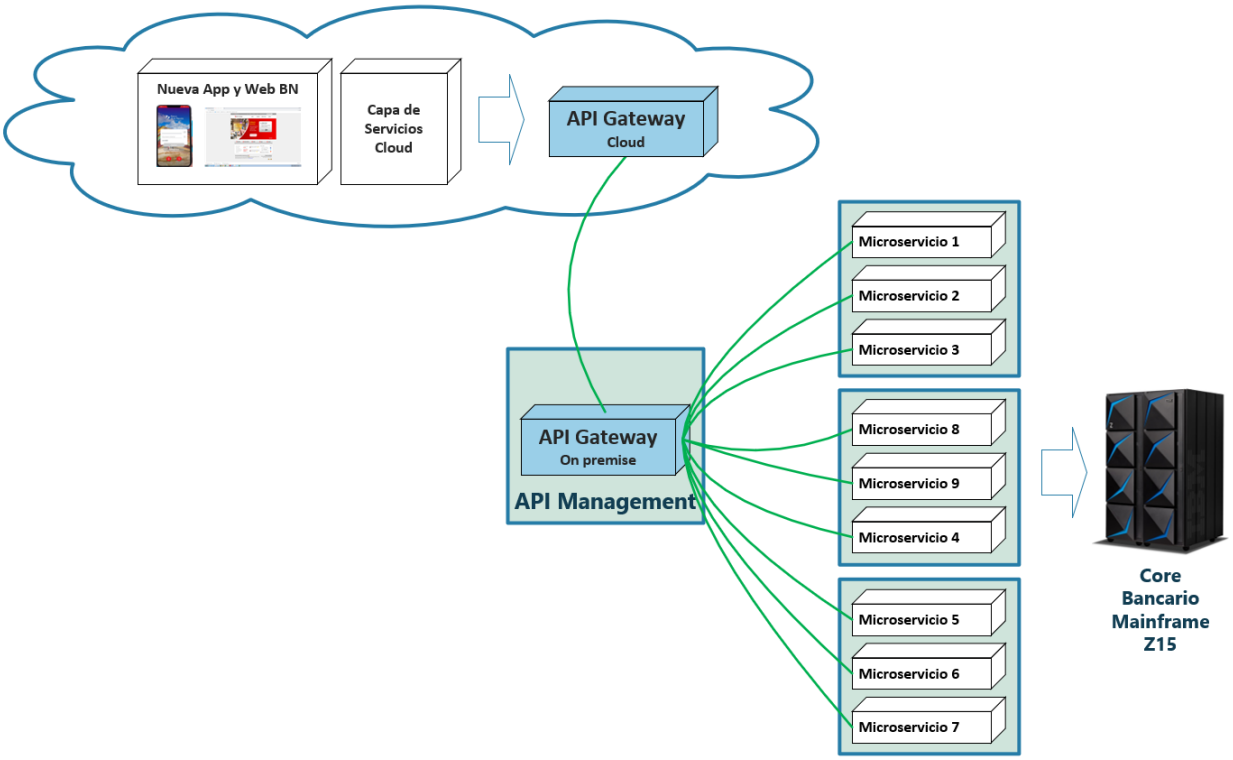


Ilustración 28: Arquitectura híbrida general

9.2. Arquitectura Tecnológica Requerida

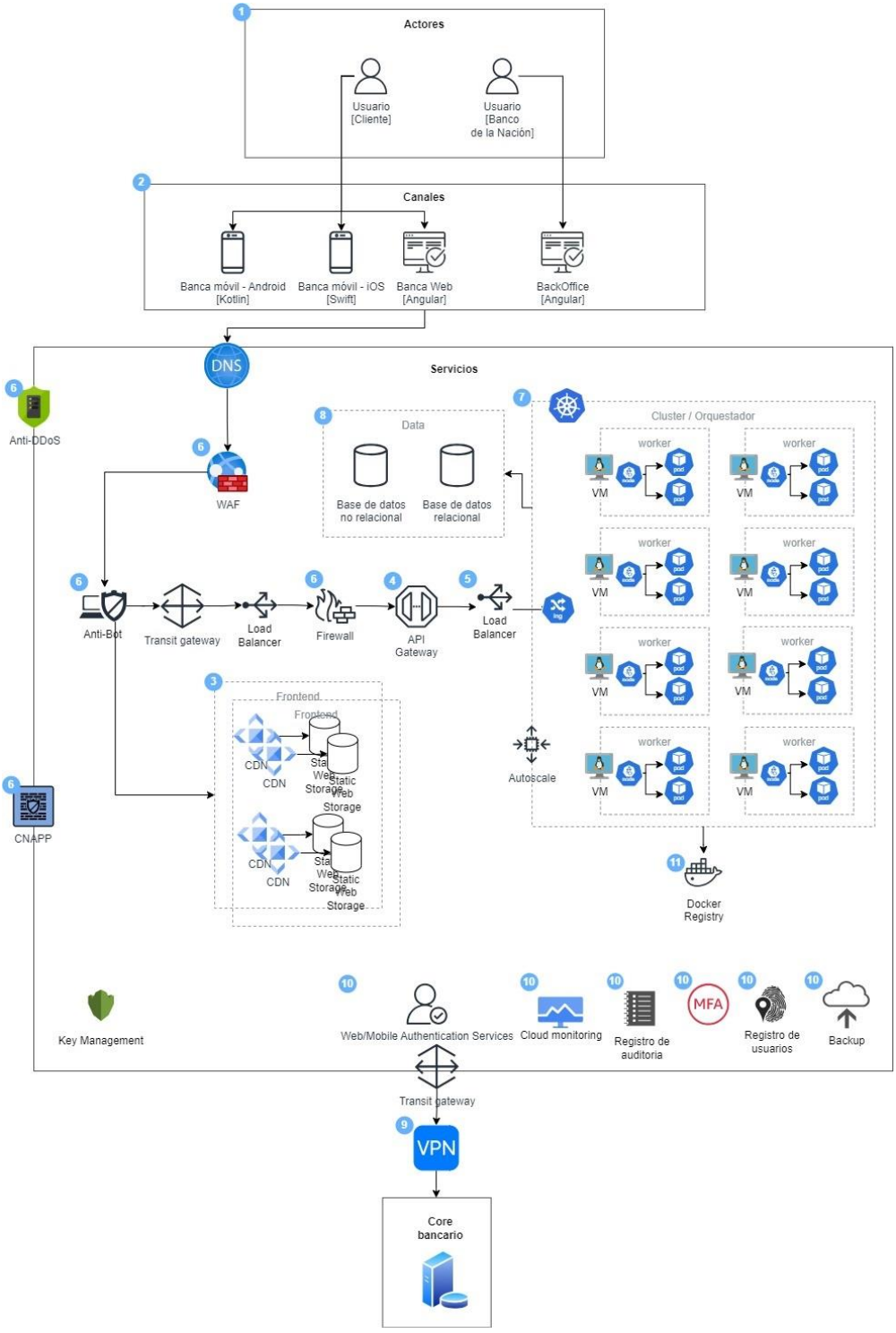


Ilustración 29: Arquitectura Tecnológica para la Banca Móvil y Banca por Internet del Banco de la Nación (diagrama referencial)

La arquitectura requerida por el BN debe tener los siguientes componentes y características:

- **Frontend:** Desarrollo para las plataformas IOS, Android y Web (HomeBanking) en la nube
- **Servicios:** Plataforma Cloud Computing dimensionable según las necesidades de la App y Web con capacidad de crecimiento a demanda.
- **Tipo:** Microservicios
- **Red Interna BN:** Core Bancario.

Una arquitectura de microservicios consta de una colección de servicios autónomos y pequeños. Cada uno de servicio es independiente y debe implementar una funcionalidad de negocio individual dentro de un contexto delimitado. Un contexto delimitado es una división natural y proporciona un límite explícito dentro del cual existe un modelo de dominio.
Los componentes indicados en el numeral 9.2. Arquitectura Tecnológica Requerida se describen a continuación de manera general:

Tabla 7: Cuadro de la Arquitectura Tecnológica Referencial de la Banca Móvil y Banca por Internet del Banco de la Nación

Capa	Alias	Tipo de servicio	Descripción	Características
1. Actores	Cliente	-		Se conecta mediante aplicación o sitio web
	Usuario (Banco de la Nación)	-		Se conecta al sitio web de BO
2. Canales	Banca Móvil – Android	-	Aplicación móvil para el SO Android.	Kotlin
	Banca Móvil – iOS	-	Aplicación móvil para el SO iOS.	Swift
	Banca Web	-	Sitio o página web de la Banca Web del Banco de la Nación.	Angular o C# sobre .NET Core Utiliza CDN

Capa	Alias	Tipo de servicio	Descripción	Características
	BackOffice	-	Sitio o página web de la plataforma BO.	Angular o C# sobre .NET Core Utiliza CDN
3. Frontend	CDN	PaaS o SaaS	Panel administrativo de las webs	Distribución de sitios web
	Static web storage	PaaS o SaaS	Servicio de almacenamiento de objetos para las webs estáticas de Banca Web y BackOffice	Repositorio para archivos de web estática
4. Redes	ApiGateway	PaaS o SaaS	Servicio Cloud de enrutamiento de servicios.	Gestión de APIs
5. Redes	Network Load balancer	PaaS o SaaS	Equilibrador de carga de red.	Servicio Cloud
6. Seguridad	WAF	SaaS	Protege de múltiples ataques al backend.	Servicio cloud o SaaS de terceros
	Anti-DDoS	SaaS	Servicio de protección contra ataques DDoS que protege las aplicaciones que se ejecutan.	Servicio cloud o SaaS de terceros

Capa	Alias	Tipo de servicio	Descripción	Características
	Firewall	SaaS	Proporciona una capa adicional de seguridad para aplicaciones web en la nube. Permite a los usuarios definir reglas personalizadas para filtrar y controlar el tráfico web, protegiendo contra amenazas como inyecciones SQL, ataques de fuerza bruta y otros.	Servicio Cloud o SaaS de terceros
	Anti-Bot	SaaS	Brinda visibilidad y control sobre bots comunes y generales que consumen recursos en exceso, sesgan las métricas, generan tiempo de inactividad o realizan otras actividades no deseadas	Servicio cloud o SaaS de terceros proporcionado por el BN
	CNAPP	SaaS	Una Plataforma de Protección de Aplicaciones de la Nube (CNAPP) todo-en-uno facilita el monitoreo, detección y acción sobre potenciales amenazas y vulnerabilidades de seguridad, mejorando la seguridad para las aplicaciones nativas de la nube a través de capacidades integradas.	Servicio cloud o SaaS de terceros

Capa	Alias	Tipo de servicio	Descripción	Características
7. Contenedores	Orquestador K8s	PaaS o SaaS	Servicio de contenedores administrado para ejecutar y escalar aplicaciones Kubernetes en la nube o en las instalaciones.	- Incluye zonas de disponibilidad y clusters de Kubernetes. - PODs con auto escalado horizontal (HPA) - Lenguaje de programación Java o C# sobre .NET Core
	VM para orquestadores (en arquitectura IaaS o PaaS)	IaaS o SaaS		
8. Base de datos	Base de datos relacional	PaaS o SaaS	Base de datos relacional del BO.	-
	Base de datos no relacional	PaaS o SaaS	Base de datos NOSQL de los logs.	-
9. Conectividad on-premise	VPN	PaaS o SaaS	Servicio para establecer un túnel de comunicación seguro con el entorno on-premise.	El BN podrá solicitar migrar a Direct Connect si la demanda transaccional lo requiere.
10. Monitoreo y registro de usuarios	Monitoreo Cloud	PaaS o SaaS	Servicio que permite monitorear los recursos y establecer alarmas para el escalamiento de recursos.	-

Capa	Alias	Tipo de servicio	Descripción	Características
	MFA	-	La autenticación multifactor (MFA) es un método de autenticación que requiere el uso de más de un factor para verificar la identidad de un usuario.	-
	Registro de usuarios	PaaS o SaaS	Permite la administración de identidades y el acceso a los servicios y recursos de la nube de manera segura.	Servicio nativo de cloud
	Backup	PaaS o SaaS	Backup de las máquinas virtuales.	-
	Autenticación de clientes	SaaS	Autenticación de Clientes para dispositivos móviles y web	Este servicio se usará a demanda. El Banco decidirá antes del Pase a Producción de manera masiva si continuará con el uso de este servicio.
11. Imágenes de Contenedores	Docker repository	PaaS o SaaS	Servicio que permite gestionar imágenes desde contenedores de Docker.	-

9.3. Gestión de Accesos e identidades

- El módulo de administración de la solución propuesta, en la fase de autenticación, deberá estar preparada para poder integrarse con la solución IBM Verifiy SaaS (servicio en nube), brindando un "Proveedor de Identidades" para realizar SSO – Single Sign On, utilizando tecnologías afines como SAML o OIDC.
- El módulo de administración de usuarios de la solución propuesta, en la fase de autorización, deberá estar preparada para poder integrarse con la solución IBM Verify Identity Manager, siendo responsabilidad del postor dicha integración. El Banco de la Nación gobierna el "aprovisionamiento automático y la gestión del ciclo de vida de la cuenta" con la solución IBM Security Verify identity Manager, por lo que la solución propuesta deberá gestionar toda la fase de autorización en su propio módulo de gestión de accesos.
- El Banco de la Nación brindará toda la información que se requiera sobre la solución de IBM Verifiy SaaS y IBM Verify Identity Manager.
- El Contratista deberá considerar la información de la arquitectura del Banco de la Nación para desarrollar el mapa de la arquitectura integral, el cual tendrá que ser actualizado en caso de existir un cambio. Además, deberá ser revisado y aprobado por el área técnica del Banco antes del despliegue de cada MVP.

9.4. Prestación del Servicio de Nube a contratar

La Infraestructura pública o Nube pública descritos en los presentes términos de referencia deberán tener una disponibilidad hasta (SLA) hasta 99.95% que equivale aproximado a 30 minutos fuera de servicio acumulados al mes. Asimismo, una latencia mínima de 150 milisegundos entre la nube y los Centros de Datos del Banco de la Nación.

El servicio deberá contar con una plataforma o consola la cual permita administrar los servicios de Infraestructura pública o Nube pública de Microservicios, la misma que será manejado por el CONTRATISTA del Servicio de Nube a contratar.

Independientemente de la modalidad de entrega del servicio para la nueva plataforma bancaria (SaaS, PaaS/SaaS o IaaS/PaaS/SaaS), todos los servicios indicados detallados entre los numerales 9.5.1 y 9.5.31 deberán ser compatibles con lo indicado en estos puntos, incluso si no se utilizan en su totalidad.

9.5. Descripción del Servicio de Nube a contratar

9.5.1. Implementación de la Arquitectura en la Nube

Con el objetivo de modernizar y optimizar nuestra infraestructura tecnológica, se establece como requisito indispensable en estos términos de referencia la contratación de un servicio especializado para la implementación

de una infraestructura en la nube. El CONTRATISTA seleccionado deberá planificar, configurar y gestionar los entornos en la nube, cumpliendo con los más altos estándares de seguridad, escalabilidad y disponibilidad. La infraestructura en la nube deberá ser capaz de soportar eficientemente nuestras operaciones, garantizando la integridad y confidencialidad de los datos. Además, se espera que el servicio contratado incluya la asesoría necesaria para una transición fluida y la capacitación de nuestro personal en la administración eficaz de la nueva infraestructura. Los ambientes a implementar serán los de Desarrollo, Pruebas y Producción.

- El proveedor de nube debe ser un proveedor de servicios de nube pública y por lo tanto debe formar parte del cuadrante de Líderes en el Cuadrante Mágico de Gartner vigente para servicios de infraestructura y plataforma en la nube.
- El participante en su oferta presentará en copia simple las siguientes certificaciones de la empresa que brindará el servicio de nube[12]:
  - ✓ PCI-DSS: Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago.
  - ✓ Cloud Security Alliance (CSA): controles de la alianza de seguridad en la nube.
  - ✓ ISO 9001: estándar de calidad internacional
  - ✓ ISO 22301: implementación, mantenimiento y mejora a sistemas de continuidad de negocio.
  - ✓ ISO 27001: controles de administración de seguridad
  - ✓ ISO 27017: controles específicos de nube
  - ✓ ISO 27018: protección de datos personales o[13] ISO 27701: sistema de gestión sobre la privacidad y gestión del contenido
  - ✓ SOC 1: informe de controles de auditoría
  - ✓ SOC 2: informe de seguridad, disponibilidad y confidencialidad
  - ✓ SOC 3: informe de controles generales

9.5.2. Servicio con Alta Disponibilidad

El CONTRATISTA implementará y asegurará que los servicios estén configurados para proporcionar eficiencia, escalabilidad, continuidad y seguridad:

- Se realizarán pruebas de alta disponibilidad conjunta que permita conocer que los canales Banca Móvil y Banca por Internet, con todos su componentes y servicios que la soportan, tanto en la nube (proveedores) como on premise (CDP y CDA del BN), pueda operar ante una interrupción o indisponibilidad de algún componente.
- La subgerencia de Producción y la Oficina de Seguridad Informática de la Gerencia de TI, realizará la prueba conjunta con el proveedor.

[12] Pliego de Consultas N° 01-2024 - Concurso de Méritos (Consulta N° 1 PERÚ APP, Consulta N° 6 PERÚ APP y Consulta N° 43 TCO LATAM).
[13] Pliego de Consultas N° 01-2024 - Concurso de Méritos (Consulta N° 1 PERÚ APP, Consulta N° 6 PERÚ APP y Consulta N° 43 TCO LATAM).

- Adicionalmente, el proveedor deberá presentar un informe de las pruebas de alta disponibilidad de la solución que validen su esquema de alta disponibilidad e indiquen la arquitectura y procedimientos que se han probado, este informe debe indicar el tiempo de recuperación producto de la prueba.
- El servicio debe contar con una infraestructura compuesta por centros de datos organizados en zonas de disponibilidad, pudiendo tener algunos componentes que por su naturaleza requieran estar en diferentes regiones o en forma Global.
- La zona de disponibilidad estará compuesta por al menos un Centro de Datos el cual proveerá capacidades de aprovisionamiento de servicios. La región permitirá interconectar al menos 2 zonas de disponibilidad para permitir brindar servicios altamente disponibles y redundantes que permitan operar de manera continua sin interrupciones de servicio, de tal forma que, ante alguna indisponibilidad de un componente, el servicio no se vea afectado. Asimismo, se realizarán pruebas de alta disponibilidad a partir de la entrega del MVP 4 y previo a su pase masivo a producción, a partir de allí, se realizará una prueba anual hasta el fin del contrato. El Banco coordinará con el Contratista las pruebas que se realizarán. Estas pruebas deberán evidenciar el uso y traslado de la carga entre las zonas de disponibilidad.
- Las coordinaciones entre el Contratista y el Banco, para las pruebas de alta disponibilidad, definirán el(los) responsable(s) en llevar a cabo dicha actividad. Esta definición se realizará en los comités del proyecto.
- El servicio debe permitir el despliegue para los servicios de cómputo y almacenamiento en diferentes zonas de disponibilidad dentro de la misma región elegida, con la finalidad que la Entidad pueda crear esquemas de continuidad de operaciones y recuperación en caso de desastre.
- El servicio debe de asegurar que los datos son almacenados única y exclusivamente en la región geográfica elegida salvo servicios que sean globales a la plataforma.
- La Gerencia de TI, realizará la prueba conjunta con el Contratista y emitirá un informe que indique con claridad la arquitectura y procedimientos que se han probado, este informe debe indicar el tiempo de recuperación producto de la prueba.
- Adicionalmente, el proveedor deberá presentar un informe de las pruebas de alta disponibilidad de la solución que validen su esquema de alta disponibilidad sobre una arquitectura Banco integral actualizada.

9.5.3. Servicio de Gestión de DNS del PSN

a. El servicio debe ser escalable y debe proveer alta disponibilidad.
b. El servicio debe permitir crear reglas de reenvío condicional y puntos de enlace DNS para resolver nombres personalizados controlados en las zonas privadas alojadas en el servicio o en los servidores DNS que se encuentran en las instalaciones.

c. El servicio debe permitir redirigir a los usuarios finales hacia los mejores puntos de enlace para la aplicación en función de la geo-proximidad, la latencia, el estado y otras consideraciones.
d. El servicio debe permitir remitir a los usuarios finales a un punto de enlace determinado que la Entidad especifique en función de la ubicación geográfica del usuario final.
e. El servicio debe permitir administrar nombres de dominio personalizados para los recursos de la nube internos sin exponer datos de DNS en la web pública.
f. El servicio debe permitir dirigir automáticamente a los visitantes del sitio web a una ubicación alternativa para evitar interrupciones del servicio.
g. El servicio debe permitir dirigir automáticamente a los visitantes del sitio web a una ubicación alternativa para evitar interrupciones del servicio.
h. El servicio debe ofrecer servicios de registro de nombres de dominio, donde sea posible buscar y registrar nombres de dominio disponibles o transferir nombres de dominio existentes para que se administren a través del servicio.
i. El servicio debe contar con una sencilla interfaz de servicios web que permita ponerse en marcha en cuestión de minutos.
j. El servicio debe permitir transferir el dominio desde otro servicio DNS al servicio DNS en la nube.
k. El servicio debe ofrecer un conjunto sencillo de API que facilita la creación y la administración de registros DNS para los dominios.

9.5.4. Servicios de Cómputo y Procesamiento del PSN

a. Permitir aprovisionar recursos de cómputo sobre Infraestructura de Nube. Las máquinas virtuales y otros recursos deben poder ejecutar los sistemas operativos Linux o Windows, las cuales deberán poder ser accesibles, escalables y fácilmente configurables ya sea mediante un panel de control manual o mediante interfaces de programación (API).
b. El proveedor/fabricante debe contar con soporte a ediciones de sistemas operativos vigentes en la plataforma de Nube:
   - Soporte Windows: Sistemas operativos compatibles con las extensiones del proveedor/fabricante.
   - Soporte Linux: Distribuciones de Linux aprobadas para el proveedor/fabricante.
c. El servicio debe contar con un entorno virtual de cómputo que permita utilizar interfaces de servicios web para lanzar recursos de cómputo con distintos sistemas operativos, cargarlas con su entorno de aplicaciones personalizado, administrar los permisos de acceso a la red y ejecutar su imagen utilizando los sistemas que desee.
d. El servicio debe permitir pausar o detener y reanudar o inicializar los recursos de cómputo de manera manual o automática de acuerdo con la configuración deseada de escalabilidad.

e. El servicio debe contar con recursos de cómputo de E/S de alto desempeño.
f. El servicio debe contar con recursos de cómputo de almacenamiento estándares de la industria como, por ejemplo: HDD, SSD y/o similares.
g. El servicio debe permitir configuraciones de CPU optimizadas.
h. El servicio debe contar con opciones de almacenamiento flexibles.
i. El servicio debe ser suministrado bajo un esquema de pago por uso.
j. El servicio debe permitir el uso de direcciones IP públicas.
k. El servicio debe permitir el uso de direcciones IP elásticas que permita asignar una IP pública a cualquiera de las máquinas virtuales.
l. El servicio debe permitir ajustar la escala de la capacidad de los recursos de cómputo automáticamente de acuerdo con las condiciones que se definan.

9.5.5. Servicios de Gestión de Identidad y Acceso del PSN

La solución de administración de identidades debe de contar con las siguientes funcionalidades y/o capacidades:

a. Contar con capacidades de acceso condicional para usuarios y dispositivos.
b. Administración de identidades centralizada y manejo de control de accesos para usuarios y administradores.
c. Administración de accesos debe estar basado en roles.
d. El servicio debe permitir controlar el acceso y los permisos a sus recursos y servicios de la nube.
e. El servicio debe permitir que se administren permisos para sus usuarios y aplicaciones.
f. El servicio debe garantizar que los usuarios no tendrán acceso a los recursos de la nube hasta que se concedan de forma explícita los permisos.
g. El servicio debe permitir crear credenciales temporales.
h. El servicio debe permitir identificar y eliminar fácilmente los permisos no utilizados.
i. El servicio debe permitir identificar cuándo se utilizó por última vez una clave de acceso para rotar claves antiguas.
j. Contar con capacidades de acceso condicional para usuarios y dispositivos.
k. Contar con capacidades de autenticación multifactor para los usuarios.
l. Administración de identidades centralizada y manejo de control de accesos para usuarios y administradores.
m. Administración de accesos debe estar basado en roles.
n. La nube debe contar con el servicio que le permita a la Entidad definir cuentas de usuario individuales con permisos en todos los recursos de la nube.

o. La nube debe contar con el servicio que permita otorgar a los funcionarios de la Entidad y a las aplicaciones acceso federado a la consola de administración.
p. El servicio debe poder integrarse a la plataforma de identidades (IDaaS) de IBM a través de federación de accesos e identidades.

9.5.6. Servicio de Gestión de Identidad y Acceso para Clientes del PSN

a. Los grupos de usuarios del servicio deben ofrecer un directorio de usuarios seguro con capacidad de escalado para gestionar millones de usuarios.
b. Los grupos de usuarios deben proporcionar perfiles de usuarios y tokens de autenticación para los usuarios que se inscriban directamente
c. Los grupos de usuarios deben proporcionar para los usuarios federados que registren con proveedores de identidades sociales o empresariales
d. El servicio debe contar con una interfaz de usuario integrada y personalizable para la inscripción y el inicio de sesión de los usuarios
e. El servicio debe utilizar SDK de Android, iOS y JavaScript para añadir páginas de inscripción e inicio de sesión de usuarios en sus aplicaciones.
f. La solución tipo CIAM - Customer identity and Access Management, deberá identificar recursos de tipo acceso público.
g. El servicio debe proporcionar autenticación flexible basada en riesgos y protección contra el uso de credenciales vulnerables
h. El servicio debe permitir que los usuarios puedan iniciar sesión mediante proveedores de identidades de redes sociales, como Google, Facebook y Amazon, y a través de proveedores de identidades empresariales, como Microsoft Active Directory mediante SAML.
i. El servicio debe permitir definir los roles y asignar usuarios a diferentes roles para que la aplicación únicamente pueda acceder a los recursos autorizados para cada usuario.
j. El servicio debe utilizar estándares habituales de administración de identidades, como OpenID Connect, OAuth 2.0 y SAML 2.0.
k. El servicio debe permitir añadir autenticación adaptativa a las aplicaciones para ayudar a proteger las cuentas de usuarios y la experiencia de los usuarios
l. El servicio debe permitir a los usuarios verificar sus identidades mediante SMS o un generador de contraseña única basada en tiempo (TOTP), como Google Authenticator.
m. Cuando el servicio detecte que el usuario ha especificado credenciales que se han visto comprometidas en otro sitio, debe solicitar que cambie la contraseña.
n. El servicio debe contar con acreditaciones PCI DSS, SOC, ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018 (o en su equivalente ISO/IEC 27701) e ISO 9001.
o. El servicio debe contar con Insensibilidad configurable entre mayúsculas y minúsculas para los alias de usuario
p. El servicio debe soportar autenticación multifactor

q. El servicio debe permitir establecer insensibilidad entre mayúsculas y minúsculas para los alias de usuario

9.5.7. Servicios de Red en Nube Privada Virtual del PSN

a. El servicio debe ser escalable y debe permitir especificar un rango de direcciones IP privadas de que sean elegidas.
b. El servicio debe permitir ampliar la nube privada virtual mediante la incorporación de intervalos IP secundarios.
c. El servicio debe permitir dividir el rango privado de direcciones IP privadas de la nube privada virtual en una o varias subredes públicas o privadas para posibilitar la ejecución de aplicaciones y la prestación de servicios en la nube privada virtual.
d. El servicio debe permitir controlar el acceso de entrada y salida desde y hacia subredes individuales por medio de listas de control de acceso.
e. El servicio debe permitir almacenar datos y definir permisos de forma que el acceso a los datos sea posible exclusivamente desde el interior de la nube privada virtual.
f. El servicio debe permitir asignar varias direcciones IP y asociar múltiples interfaces de red elásticas a instancias de la nube privada virtual.
g. El servicio debe permitir asociar una o más direcciones IP elásticas a cualquier instancia de la nube privada virtual, de modo que puedan alcanzarse directamente desde Internet.
h. El servicio debe permitir conectarse a la nube privada virtual con otras nubes privadas virtuales y obtener acceso a los recursos de otras nubes privadas virtuales a través de direcciones IP privadas mediante la interconexión de nube privada virtual.
i. El servicio debe permitir conectarse de manera privada a los servicios del PSN sin usar una gateway de Internet, ni una NAT ni un proxy de firewall mediante un punto de enlace de la nube privada virtual.
j. El servicio debe permitir conectarse de manera privada a sus propios servicios o soluciones de SaaS con tecnología de PrivateLink.
k. El servicio debe permitir conectar la nube privada virtual y la infraestructura de TI local con la VPN del PSN de sitio a sitio.
l. El servicio debe permitir asociar grupos de seguridad de la nube privada virtual con instancias en la plataforma.
m. El servicio debe permitir registrar información sobre el tráfico de red que entra y sale de las interfaces de red de la nube privada virtual.
n. El servicio debe permitir habilitar IPv4 e IPv6 en la nube privada virtual.
o. El servicio debe permitir usar la replicación de tráfico de nube privada virtual a fin de capturar y replicar el tráfico de la red para las instancias.
p. El servicio debe permitir interceptar y analizar el tráfico de entrada y salida, mediante un dispositivo de red y seguridad, incluidas las ofertas de terceros.
q. El servicio debe tener la habilidad de mover direcciones entre instancias

r. El servicio debe tener la capacidad de usar nuestra propia dirección IP pública dentro de la red virtual
s. El servicio debe tener la capacidad de reflejar el tráfico y transmitirlo a un recopilador de paquetes de red.
t. El servicio debe tener la capacidad de análisis para monitoreo de trafico de red.
u. El servicio debe tener la capacidad de mover interfaces de red entre instancias
v. El servicio debe permitir implementar conectividad de tránsito (modelo Hub-and-Spoke)
w. El servicio debe permitir compartir una red virtual entre diferentes cuentas (modelo compartido)
x. El servicio debe ofrecer resolución de DNS para entornos híbridos
y. El servicio debe ofrecer resolución de DNS a nombres de host privados
z. El servicio debe ofrecer resolución de DNS a nombres de host públicos
aa. El servicio debe contar con métricas de rendimiento de la red de instancias
bb. NIC: el servicio debe contar con la capacidad para configurar comprobaciones de origen / destino en interfaces de red
cc. El servicio debe permitir el cifrado de tráfico WAN (entre los centros de datos)
dd. El servicio debe tener la habilidad de generar una red virtual de forma automática.

9.5.8. Servicios de Almacenamiento de Bloques del PSN

a. Permitir crear unidades de almacenamiento que puedan ser montadas en: Infraestructura como servicios (IaaS) y/o Plataforma como servicio (PaaS).
b. El servicio debe permitir crear volúmenes de almacenamiento y adjuntarlos a recursos de cómputo.
c. El servicio debe permitir crear un sistema de archivos sobre estos volúmenes, ejecutar una base de datos o darles cualquier otro uso que le daría al almacenamiento en bloques.
d. El servicio debe permitir optimizar el rendimiento del almacenamiento y los costos de la carga de trabajo.
e. El servicio debe ofrecer almacenamiento respaldado por SSD para cargas de trabajo transaccionales como bases de datos y/o volúmenes de arranque (el rendimiento depende principalmente de las IOPS) y almacenamiento respaldado por HDD para cargas de trabajo intensivas como el procesamiento de registros (el rendimiento depende principalmente de los MB/s).
f. El servicio debe permitir aumentar la capacidad, ajustar el rendimiento y modificar el tipo de cualquier volumen de generación nueva o existente de manera dinámica y sin interrupciones ni impactos en el rendimiento.
g. El servicio debe estar diseñado para ofrecer una alta disponibilidad y fiabilidad a través de las múltiples copias distribuidas en diferentes ubicaciones.

h. El servicio debe permitir hacer un cifrado integral de las instantáneas, los volúmenes de arranque y los volúmenes de datos.

9.5.9. Servicio de Base de Datos Relacional del PSN

a. Permitir aprovisionar plataforma como servicio (PaaS) de base de datos relacional y no relacional.
b. Permitir escalar estos servicios ya sea en espacio de almacenamiento o cómputo, de manera rápida y bajo demanda. Se espera iniciar el servicio con una demanda diaria de 2 millones de transacciones.
c. El servicio debe estar en capacidad de desarrollar tareas habituales de las bases de datos, como el aprovisionamiento, las revisiones, las copias de seguridad, la recuperación, la detección de errores y la reparación.
d. El servicio debe permitir ejecutar cargas de trabajo críticas con alta disponibilidad y conmutación por error automatizada e integrada desde la base de datos principal a una base de datos secundaria replicada sincrónicamente.
e. Los recursos de cómputo de base de datos deben estar preconfigurados con los parámetros y ajustes adecuados para el motor y la clase que se haya seleccionado.
f. El servicio debe permitir configurar la aplicación automática de parches de software.
g. El servicio debe permitir escalar los recursos informáticos y de memoria para ampliar y/o reducir la implementación del servicio.
h. El servicio debe permitir aprovisionar almacenamiento adicional según aumenten los requisitos.
i. El servicio debe permitir crear una o varias réplicas de un recurso de cómputo de base de datos de origen determinada y abastecer el alto volumen de tráfico de lectura de la aplicación desde distintas copias de sus datos, lo cual debe mejorar el rendimiento de lectura total.
j. El servicio debe permitir la creación de copias de seguridad automatizadas para poder hacer una recuperación a un momento dado de la base de datos.
k. El periodo de retención de copia de seguridad se debe poder configurar hasta un máximo de 35 días.
l. El servicio debe permitir crear instancias de la base de datos y conservarlas hasta cuando se requiera.
m. El servicio se debe poder desplegar en múltiples ubicaciones para mejorar la disponibilidad y durabilidad de la base de datos.
n. El servicio debe contar con la capacidad de controlar las acciones que los usuarios y grupos pueden realizar en recursos específicos.
o. El servicio debe permitir monitorear métricas operativas clave, incluidos el uso de la capacidad de cómputo, memoria y almacenamiento, la actividad de E/S y las conexiones de recursos de cómputo de bases de datos.
p. El servicio debe poder notificar eventos de la base de datos por email o SMS (se requiere un mínimo de 30,000 SMS mensuales).

q. El servicio debe permitir registrar y auditar los cambios en la configuración de los recursos de cómputo de base de datos, incluidos grupos de parámetros, grupos de subred, instantáneas, grupos de seguridad y suscripciones a eventos.
r. El servicio debe permitir encriptación en reposo con llaves de encriptación gestionadas por la ENTIDAD.
s. El servicio debe permitir el escalamiento vertical y horizontal.

9.5.10. Servicio de Almacenamiento de Objetos del PSN

a. El servicio debe permitir que un solo objeto pueda tener un tamaño de hasta 5 terabytes
b. El servicio debe contar con capacidades para anexar etiquetas de metadatos a los objetos, mover y almacenar datos entre los tipos de almacenamiento, configurar y aplicar controles de acceso a datos, proteger los datos frente a usuarios no autorizados, ejecutar análisis de Big Data y monitorear los datos en los niveles de objeto y carpetas que contienen objetos.
c. El servicio debe permitir el acceso a los objetos a través de los puntos de acceso del servicio o directamente a través del nombre de host de la carpeta que los almacena.
d. El servicio debe permitir anexar a cada objeto hasta 10 pares de clave-valor denominados etiquetas de objetos, que se pueden crear, actualizar y eliminar a lo largo de todo el ciclo de vida de los objetos.
e. El servicio debe permitir utilizar un informe de inventario, donde se enumeran los objetos almacenados en una carpeta de objetos o con un prefijo específico, así como sus metadatos y estado de cifrado correspondientes.
f. El servicio debe permitir copiar objetos entre carpetas, reemplazar conjuntos de etiquetas de objetos, modificar los controles de acceso y restaurar objetos archivados desde otros servicios de almacenamiento.
g. El servicio debe admitir características que ayudan a mantener el control de versiones de los datos, impedir el borrado accidental y replicar datos en diversas ubicaciones del PSN.
h. El servicio debe contar con control de versiones que permitan preservar, recuperar y restaurar fácilmente todas las versiones de un objeto almacenado, lo que debe permitir recuperarse fácilmente de acciones de usuarios involuntarias y de errores de aplicaciones.
i. El servicio debe impedir el borrado accidental al contar con funcionalidades de eliminación Multi-Factor Authentication (MFA).
j. El servicio debe permitir replicar objetos (así como sus metadatos y etiquetas de objeto respectivos) en otras regiones del PSN o en la misma ubicación para lograr una latencia reducida, conformidad, seguridad y recuperación de desastres.
k. El servicio debe permitir aplicar políticas de escritura única y lectura múltiple (WORM)

l. El servicio debe permitir aplicar etiquetas a las carpetas para asignar costos en múltiples dimensiones de negocio (por ejemplo, centros de costos, nombres de aplicación o propietarios) y, después, debe permitir utilizar los informes de asignación de costos para ver el uso y los costos que agregan las etiquetas de las carpetas.
m. El servicio debe permitir hacer el seguimiento de las actividades de nivel de carpetas y objeto e informar sobre ellas.
n. El servicio debe permitir configurar las notificaciones de eventos para activar flujos de trabajo y alertas.
o. El servicio debe permitir crear usuarios y administrar su correspondiente acceso.
p. El servicio debe conceder acceso a objetos individuales a los usuarios autorizados.
q. El servicio debe permitir configurar permisos para todos los objetos de una única carpeta.
r. El servicio debe permitir simplificar la administración del acceso de datos a conjuntos de datos compartidos creando puntos de acceso con nombres y permisos específicos para cada aplicación o conjuntos de aplicaciones.
s. El servicio debe conceder acceso a otros usuarios por tiempo limitado con direcciones URL temporales.
t. El servicio debe permitir enumerar las solicitudes realizadas a sus recursos para obtener total visibilidad de quién obtiene acceso a los distintos datos.
u. El servicio debe ofrecer características de seguridad flexibles para bloquear el acceso de usuarios no autorizados a sus datos.
v. El servicio debe admitir el cifrado tanto del lado de servidor (con tres opciones de administración clave) como del lado de cliente para cargas de datos.
w. El servicio debe permitir comprobar el estado de cifrado de los objetos
x. El servicio debe contar con controles de seguridad que garantizan que las carpetas y objetos no tengan acceso público.
y. El servicio debe contar con clases de almacenamiento: clase / nivel de almacenamiento de movimiento de datos automático basado en patrones de acceso.
z. El servicio debe contar con la siguiente funcionalidad para protección de datos: sincronización de replicación bidireccional.
aa. El servicio debe contar con la siguiente funcionalidad para protección de datos: cumplimiento de bloqueo WORM a nivel de carpeta/contenedor de objetos.
bb. El servicio debe permitir ejecutar operaciones por lotes en etiquetas, incluidas eliminaciones.
cc. El servicio debe permitir eliminar de varios objetos mediante una única llamada a la API.
dd. El servicio debe permitir agregar etiquetas a los objetos.
ee. El servicio debe permitir definir puntos de acceso para puntos de entrada seguros a datos compartidos.

ff. El servicio debe contar con una función / herramienta / servicio para analizador el acceso.
gg. El servicio debe permitir bloquear el acceso público a nivel de cuenta / suscripción.
hh. El servicio debe permitir la auditoría continua de políticas de acceso y configuración de seguridad.

9.5.11. Servicio de Red de Distribución de Contenido del PSN

a. El servicio debe permitir distribuir a clientes globalmente datos, vídeos, aplicaciones y API de forma segura, con baja latencia, altas velocidades de transferencia y dentro de un entorno fácil para desarrolladores.
b. El servicio permite entregar su contenido, sus API o sus aplicaciones a través de SSL/TLS y las características avanzadas de SSL se deben poder activar automáticamente.
c. El servicio debe permitir implementar la protección frente a ataques a la red y la capa de aplicación al integrarse con otros servicios.
d. El servicio debe soportar cifrados de SSL/TLS y HTTPS.
e. El servicio debe permitir utilizar SSD cifrados para ubicaciones de borde y volúmenes de almacenamiento elástico de bloques cifrados para cachés de borde regionales.
f. El servicio debe permitir cifrar los datos en tránsito.
g. El servicio debe soportar encriptación a nivel de campos.
h. El servicio debe restringir el acceso a su contenido con una serie de funciones.
i. El servicio debe permitir la autenticación de tokens para restringir el acceso solo a los espectadores autenticados.
j. El servicio debe evitar que usuarios de ubicaciones geográficas específicas obtengan acceso a contenido.
k. El servicio debe permitir configurar varios orígenes para habilitar la redundancia en su arquitectura de backend.
l. El servicio debe permitir medir continuamente la conectividad a Internet, el rendimiento y la computación para encontrar la mejor manera de direccionar las solicitudes a nuestra red, teniendo en cuenta el rendimiento, la carga, el estado operativo y otros factores para ofrecer la mejor experiencia en tiempo real.
m. El servicio debe permitir la transmisión eficiente de solicitudes entre las ubicaciones.
n. El servicio debe permitir acelerar tanto el contenido estático como el dinámico para mejorar el rendimiento de los usuarios.
o. El servicio debe proporcionar una gran flexibilidad para optimizar el comportamiento de la caché, junto con optimizaciones de la capa de red para la latencia y el rendimiento.
p. El servicio debe admitir el protocolo WebSocket, así como el protocolo HTTP con los siguientes métodos HTTP: GET, HEAD, POST, PUT, DELETE, OPTIONS y PATCH.

q. El servicio debe permitir mejorar el rendimiento de los sitios web dinámicos que incluyen formularios web, espacio para comentarios, cuadros de inicio de sesión, botones "añadir a la cesta", aplicaciones basadas en WebSocket y otras características que cargan datos procedentes de los usuarios finales
r. El servicio debe permitir utilizar un único nombre de dominio para la entrega de todo el sitio web y así acelerar tanto la descarga como la carga de partes de su sitio web.
s. El servicio debe permitir técnicas como el almacenamiento en caché por capas y la optimización de la desduplicación de objetos en caché para ayudar a maximizar la retención de caché.
t. El servicio debe contar con registros de actividades en tiempo real.
u. El servicio debe permitir crear / renovar certificados públicos / privados de forma gratuita.

9.5.12. Servicios de Balanceo de Carga del PSN

a. El servicio debe distribuir automáticamente el tráfico de aplicaciones entrantes a través de varios destinos, tales como instancias y direcciones IP.
b. El servicio debe estar en capacidad de detectar destinos que funcionen incorrectamente, dejar de enviar tráfico a ellos y, a continuación, distribuir la carga entre los destinos restantes que no presenten problemas.
c. Se deben poder crear y administrar grupos de seguridad asociados con balanceadores de carga a fin de ofrecer opciones de seguridad y redes adicionales.
d. El servicio debe proporcionar la capacidad de administración integrada de certificados y descifrado SSL/TLS, lo que debe brindar la flexibilidad para administrar de manera centralizada los parámetros de SSL del balanceador de carga y eliminar el trabajo intensivo de la CPU de la aplicación.
e. El servicio debe permitir equilibrar cargas de trabajo a nivel de capa 4 y capa 7.
f. El servicio debe permitir equilibrar la carga en aplicaciones HTTP o HTTPS para características específicas de la capa 7.
g. El servicio debe facilitar el monitoreo de rendimiento de las aplicaciones en tiempo real.
h. El servicio debe proporcionar direccionamiento de solicitudes avanzado destinado a la entrega de arquitecturas de aplicaciones modernas, incluidos microservicios y aplicaciones basadas en contenedores.
i. El servicio debe asegurar que se utilicen en todo momento los protocolos y cifradores SSL/TLS más recientes.
j. El servicio debe permitir equilibrar cargas a un backend de aplicación alojado en cualquier dirección IP y con cualquier interfaz de una instancia.
k. El servicio debe permitir usar direcciones IP como destinos para equilibrar cargas de aplicaciones alojadas en ubicaciones locales.

l. El servicio debe permitir distribuir el tráfico de entrada entre destinos en numerosas zonas de disponibilidad.
m. El servicio debe escalar automáticamente la capacidad de administración de solicitudes como respuesta al tráfico de aplicaciones entrante.
n. El servicio debe poder ser configurado para que se pueda obtener acceso a él desde Internet o crear un balanceador de carga sin direcciones IP públicas para que actúe como balanceador de carga interno (es decir, sin acceso a Internet).
o. Si la aplicación se compone de varios servicios individuales, el balanceador de carga de aplicaciones debe poder direccionar una solicitud a un servicio en función del contenido de la solicitud.
p. El servicio debe soportar: direccionamiento basado en host, direccionamiento basado en ruta, direccionamiento basado en el encabezado HTTP, direccionamiento basado en el método HTTP, direccionamiento basado en parámetros de cadenas de consultas y direccionamiento basado en CIDR para direcciones IP de origen.
q. El servicio debe poder direccionar una solicitud de cliente basada en el CIDR para direcciones IP de origen desde donde se origina la solicitud.
r. El servicio debe ser compatible con HTTP/2.
s. El servicio debe ser compatible con WebSockets.
t. El servicio debe contar con compatibilidad IPv6 nativa.
u. El servicio debe ser compatible con las sesiones persistentes mediante el uso de cookies generadas por el balanceador de carga.
v. El servicio debe direccionar el tráfico solamente a destinos que funcionan correctamente.
w. El servicio debe facilitar el monitoreo de métricas tales como el recuento de solicitudes, el recuento de errores, los tipos de errores y la latencia de las solicitudes.
x. El servicio debe permitir registrar todas las solicitudes enviadas al balanceador de carga.
y. El servicio debe permitir monitorear una solicitud por un ID único a medida que esta se desplaza por los diversos servicios que componen sus sitios web y aplicaciones distribuidas.
z. El servicio debe ser compatible con un algoritmo de equilibrio de cargas de turno rotativo.
aa. El servicio debe permitir autenticar a los usuarios de manera segura a medida que obtengan acceso a las aplicaciones de la nube.
bb. El servicio debe permitir permite a los usuarios finales realizar autenticaciones mediante proveedores de identidades de redes sociales y mediante proveedores de identidades empresariales, como Microsoft Active Directory a través de SAML o cualquier proveedor de identidades que cumpla con OpenID Connect (IdP).
cc. El servicio debe permitir redirigir una solicitud entrante de una URL a otra distinta.

dd. El servicio debe tener la capacidad de redirigir las solicitudes de HTTP a las solicitudes de HTTPS.

9.5.13. Servicios VPN Site-to-Site del PSN

a. El servicio debe permitir establecer conexiones seguras entre sus redes en las instalaciones de la Entidad, las oficinas remotas, los dispositivos y la red global del proveedor de nube.
b. El servicio permite acceder ya sea con una configuración de IP Security (IPSec) de Site-to-Site VPN o con un túnel de protocolo seguridad de la capa de transporte (TLS) de Client VPN.
c. El servicio soporta la conexión tanto de la gateway privada virtual como de Transit Gateway.
d. El tráfico en el túnel entre los puntos de enlace debe poder encriptarse con AES128 o AES256 y utilizar protocolos Diffie-Hellman para intercambios claves.
e. Para Site-to-Site VPN se debe autenticar mediante funciones SHA1 o SHA2.
f. El servicio debe brindar opciones de túnel personalizables, incluidos dirección IP de túnel interna, clave compartida previamente y número de sistema autónomo para protocolo de gateway fronteriza (BGP ASN).
g. El servicio debe contar con disponibilidad de rutas múltiples de igual costo (ECMP) con Site-to-Site VPN en la Transit Gateway para ayudar a incrementar la banda ancha de tráfico en varias rutas.
h. Site-to-Site VPN debe soportar aplicaciones trasversales de NAT, de modo que pueda utilizar direcciones IP privadas, en redes privadas, detrás de enrutadores con una sola dirección IP pública con conexión a Internet.
i. Site-to-Site VPN debe permitir enviar métricas al servicio de monitoreo para ofrecer mayor visibilidad y supervisión.
j. Site-to-Site VPN debe soportar el uso de certificados privados.
k. Site-to-Site VPN debe soportar encriptación IKE, IPsec y TLS.
l. El servicio debe permitir mejorar el rendimiento de sus conexiones Site-to-Site VPN reduciendo la distancia mediante la cual se comparten los datos en Internet y, preferiblemente, sacando provecho de la fiabilidad y el rendimiento de la red de fibra global del proveedor de nube.

9.5.14. Transit Gateway del PSN

a. El servicio debe permitir conectar la nube y las redes locales a través de un eje central.
b. El servicio debe actuar como un enrutador en la nube: cada conexión nueva se realiza solo una vez.
c. Los datos se deben cifrar automáticamente y nunca deben viajar a través de la Internet pública.
d. El servicio debe tener una vista única de toda su red, incluso se debe poder conectar a dispositivos de red de área amplia definida por software (SD-WAN).

e. El servicio debe ser compatible con el direccionamiento dinámico y estático de la capa 3 la nube y la VPN.
f. El servicio debe permitir crear conexiones de VPN entre Transit Gateway y las gateways locales mediante con una VPN.
g. El servicio debe permitir crear múltiples varias VPN que anuncien los mismos prefijos y habilitar rutas múltiples de igual costo (Equal Cost Multipath, ECMP) entre estas conexiones. Al balancear la carga del tráfico en varias rutas, ECMP debe permitir aumentar el ancho de banda.
h. El servicio debe permitir la integración nativa de los dispositivos de Red de área amplia definida por software (SD-WAN) en la nube.
i. El servicio debe permitir ampliar el borde SD-WAN a la nube mediante protocolos estándar como Generic Routing Encapsulation (GRE) y protocolo de gateway fronteriza (BGP).
j. El servicio debe admitir direccionamiento dinámico con mayor nivel de límites de ruta, por lo que se elimina la necesidad de establecer múltiples VPN IPsec entre los dispositivos SD-WAN y Transit Gateway.
k. El servicio debe permitir la resolución de nombres de host DNS públicos en direcciones IP privadas cuando se consultan desde la nube.
l. El servicio debe proporcionar estadísticas y registros que luego serán utilizados por servicios como registros de flujo.
m. El Administrador de red del servicio debe incluir eventos y métricas para supervisar la calidad de la red global, tanto en la nube como en las instalaciones.
n. El servicio debe permitir usar la interfaz de línea de comandos y la consola para crear y administrarlo.
o. El servicio debe proporcionar métricas como la cantidad de bytes enviados y recibidos entre la nube y las VPN, el recuento de paquetes y de caídas.
p. El servicio debe permitir usar registros de flujo para obtener información sobre el tráfico de IP que pasa a través de la conexión.
q. El servicio debe facilitar establecer interconexiones entre gateways de tránsito en la misma región de la nube o en entre regiones.
r. La interconexión debe permitir dirigir directamente el tráfico entre dos gateways de tránsito.
s. El servicio debe permitir crear y administrar fácilmente grupos de multidifusión en la nube.
t. El servicio debe permitir escalar verticalmente y horizontalmente la solución de multidifusión en la nube para distribuir simultáneamente un stream de contenido a varios suscriptores.
u. El servicio debe brindar un control específico sobre quién puede producir y quién puede consumir tráfico de multidifusión.
v. El servicio debe soportar que se administre el acceso de forma segura.
w. El administrador de red debe identificar automáticamente las conexiones VPN de sitio a sitio y los recursos en las instalaciones con los que están asociados.

x. El servicio debe permitir definir manualmente la red en las instalaciones en el administrador de red de Transit Gateway.
y. El servicio debe permitir recibir notificaciones de cambios en la red, cambios en el direccionamiento y actualizaciones del estado de la conexión.
z. El servicio debe permitir supervisar la red global a través de métricas de rendimiento y tráfico, como los bytes de entrada y salida, los paquetes de entrada y salida y los paquetes eliminados.
aa. El servicio debe ser compatible con Cisco, Aruba, Silver Peak, Aviatrix y Versa.
bb. El servicio debe permitir obtener una vista unificada de la red en la nube y en las instalaciones.
cc. El servicio debe soportar IPv6.
dd. El servicio debe tener capacidades de segmentación de red.
ee. El servicio debe soportar una lista de prefijos administrados; es decir, un conjunto de uno o más bloques CIDR.
ff. El servicio debe permitir realizar análisis de ruta en Transit Gateways en redes globales.
gg. El servicio debe soportar ruteo estático.
hh. El servicio debe contar con integración nativa SD-WAN.
ii. El servicio debe soportar el balanceo entre múltiples conexiones de VPN.

9.5.15. Servicio de Conexión de Red Directo del PSN

a. El servicio debe estar disponible en ubicaciones internacionales para garantizar que sea posible realizar conexiones próximas a donde las necesite RTVC.
b. El servicio debe ofrecer velocidades de conexión e de entre 50 Mbps hasta 100 Gbps.
c. El servicio debe ofrecer opciones de cifrado.
d. El servicio debe contar con cifrado nativo IEEE 802.1AE (MACsec) punto a punto en ubicaciones específicas.
e. El servicio debe ofrecer la opción de Site to Site VPN para conexiones seguras mediante Ipsec.
f. El servicio debe permitir crear conexiones de red privadas integrales entre las oficinas, los centros de datos y las instalaciones de co-ubicación.
g. El servicio debe permitir crear enlaces mediante un puerto Ethernet de 1 Gbps, 10 Gbps o 100 Gbps.
h. El servicio debe contar con capacidad para configurar el Número de Sistema Autónomo (ASN) en el lado de la nube (BYOASN).
i. El servicio debe soportar control de salida preciso para el tráfico privado.
j. El servicio debe permitir agrupar múltiples enlaces en una sola conexión con mayor ancho de banda.
k. El servicio debe soportar IPv6.
l. El servicio debe soportar conectividad privada a la infraestructura del proveedor de la nube, en todas las regiones.

m. El servicio debe contar con un kit de herramientas de resiliencia - Pruebas de conmutación por error.

9.5.16. Servicios de Monitoreo del PSN

a. El servicio debe permitir monitorear aplicaciones y recursos de infraestructura locales, híbridos y de la nube.
b. El servicio debe permitir recopilar y obtener acceso a todos los datos de rendimiento y operaciones en formato de registros y métricas a partir de una sola plataforma.
c. El servicio debe ofrecer visibilidad de hasta 1 segundo de las métricas y los datos de los registros, 15 meses de retención de datos (métricas) y la capacidad para realizar cálculos con las métricas.
d. El servicio debe permitir visualizar y analizar el estado, el rendimiento y la disponibilidad de sus aplicaciones en un solo lugar.
e. El servicio debe tener la capacidad de contar una visión completa de las aplicaciones y sus dependencias.
f. El servicio debe tener la capacidad de hacer monitoreo de las aplicaciones en tres dimensiones: monitoreo de infraestructura (con métricas y registros para comprender los recursos que respaldan sus aplicaciones), monitoreo de transacciones (con rastreos para comprender las dependencias entre sus recursos) y monitoreo de usuario final (para monitorear sus puntos de enlace y notificarle cuando su experiencia de usuario final se haya degradado).
g. El servicio debe permitir monitorear puntos de enlace de la aplicación.
h. El servicio debe permitir escribir reglas para indicar los eventos de interés para la aplicación y las acciones automatizadas que se deben desencadenar cuando una regla concuerde con un evento.
i. El servicio debe facilitar el diagnóstico, aislamiento y corrección de problemas.
j. El servicio debe permitir realizar análisis históricos para optimizar costos y obtener información en tiempo real sobre los recursos de la infraestructura y la optimización de las aplicaciones.
k. El servicio debe permitir recopilar hasta 50 métricas predeterminadas de servicios de la nube.
l. El servicio debe permitir crear gráficos reutilizables y ver las aplicaciones y los recursos de la nube en una vista unificada.
m. El servicio debe permitir monitorear contenedores.
n. El servicio debe contar con granularidad configurable de monitoreo/alerta.
o. El servicio debe permitir correlacionar el patrón de registros de una métrica específica y definir alarmas para que avisen de manera proactiva acerca de problemas operativos y de rendimiento.
p. La funcionalidad de alarmas debe permitir definir un umbral de métricas y activar una acción.
q. El servicio debe permitir hacer correlaciones entre registros y métricas.
r. El servicio debe contar con mecanismos de búsqueda.

s. El servicio debe admitir el uso de percentiles.
t. El servicio debe permitir monitorear el rendimiento operativo, resolver errores y detectar tendencias.
u. El servicio debe permitir minimizar los tiempos de inactividad y el potencial impacto en el desempeño de la solución.
v. El servicio aplica algoritmos de aprendizaje automático para analizar los datos de las métricas de manera permanente y detectar los comportamientos anormales.
w. El servicio debe permitir controlar qué usuarios y recursos tienen permiso para obtener acceso a sus datos y de qué manera lo hacen.
x. El servicio debe permitir cifrar los datos en tránsito y en reposo.

9.5.17. Servicio de Gestión de Claves en la Nube del PSN

a. El servicio debe permitir crear y administrar con facilidad las claves y controlar el uso del cifrado en una amplia variedad de servicios de la nube y en las aplicaciones.
b. El servicio debe contar con módulos de seguridad de hardware que sirvan para proteger las claves y que han sido validados según las normas FIPS 140-2, o están en proceso de validación.
c. El servicio debe permitir agregar de manera sencilla funcionalidades de cifrado y firma digital en el código de la aplicación.
d. El servicio debe tener la capacidad de ejercer un control centralizado del ciclo de vida y los permisos de las claves.
e. El servicio debe permitir importar claves desde una infraestructura de administración de claves propia o utilizar las claves almacenadas.
f. El servicio debe permitir seleccionar la rotación automática anual de claves maestras generadas para no tener que volver a cifrar datos que ya lo estaban.
g. El servicio debe conservar de manera automática versiones anteriores de la clave maestra para descifrar datos cifrados con antelación.
h. El servicio debe permitir administrar las claves maestras y auditar su uso desde la consola de administración de la nube o desde una interfaz de línea de comandos.
i. El servicio de gestión de llaves se debe poder integrar con otros servicios de la nube.
j. El servicio debe soportar la ejecución de auditorías; es decir, cada solicitud que se haga en el servicio se debe anotar en un registro. La información registrada debe incluir los detalles del usuario, la hora, la fecha, la acción de API y, cuando corresponda, la clave utilizada.
k. El servicio debe ser totalmente administrado.
l. El servicio debe poder escalar automáticamente según se requiera.
m. El servicio debe almacenar varias copias de las versiones cifradas de las claves en sistemas diseñados para ofrecer una durabilidad del 99,999999999%, a fin de garantizar que la disponibilidad de las claves y los datos sea alta.

n. El servicio debe soportar la creación automáticamente copias de seguridad de las copias cifradas de las claves con el fin de mantener control total sobre el proceso de recuperación.
o. El servicio debe permitir crear un almacenamiento de claves propio con HSM.
p. El servicio debe ofrecer la posibilidad de crear y usar Customer Master Keys (CMK) asimétricas.
q. El servicio debe permitir generar un par de claves de datos asimétricas. La operación debe devolver una copia con texto no cifrado de la clave pública y la clave privada, así como también una copia de la clave privada cifrada con una CMK simétrica que se especifique.
r. El servicio debe permitir usar clave privada o pública con texto no cifrado en la aplicación local y almacenar la copia cifrada de la clave privada para un uso futuro.
s. El servicio debe permitir generar/administrar/importar llaves de cifrado simétricas (por ejemplo, AES, DES, 3DES) y asimétricas (RSA, ECC, DH) para la solución propuesta en la nube.

9.5.18. Servicio para Registro y Auditoria del PSN

a. El servicio debe permitir visualizar y registrar actividades en la cuenta de nube.
b. El servicio debe permitir obtener registros agregados de varias cuentas de la nube.
c. El servicio debe permitir visualizar y descargar registros con hasta 90 días de antigüedad.
d. El servicio debe permitir comprimir los archivos de registros.
e. El servicio debe permitir visualizar, buscar y descargar registros de actividades de las cuentas.
f. El servicio debe permitir establecer si los archivos de registro no han sido alterados, tienen algún cambio o han sido borrados.
g. El servicio debe garantizar que los registros son encriptados usando server-side encryption (SSE).
h. El servicio debe contar con capacidad para registrar actividades informáticas de borde.
i. Servicio de computación sin servidor.
j. El servicio debe permitir ejecutar código en respuesta a eventos y administra automáticamente los recursos informáticos subyacentes.
k. El servicio debe permitir ampliar la funcionalidad de otros productos del PSN con lógica personalizada o bien crear servicios back-end propios que funcionen con el nivel de seguridad, rendimiento y escala de la nube pública.
l. El servicio debe permitir ejecutar código automáticamente en respuesta a varios eventos, como solicitudes HTTP a través de un API Gateway, modificaciones realizadas en objetos contenidos en carpetas en el servicio de almacenamiento; entre otros.

m. El servicio debe estar implementado sobre infraestructura informática de alta disponibilidad donde el PSN se encarga de la administración integral de los recursos informáticos, incluido el mantenimiento del servidor y del sistema operativo, el aprovisionamiento de capacidad y el escalado automático, la implementación de parches de seguridad y código, así como la monitorización de código y los registros.
n. El servicio debe permitir crear funciones.
o. El servicio debe permitir cargar código.
p. El servicio debe permitir compilar el código.
q. El servicio debe permitir activar otros servicios ofrecidos por el PSN.
r. El servicio debe permitir usar cualquier biblioteca de terceros e incluso las nativas.
s. El servicio debe permitir empaquetar cualquier código (marcos, SDK, bibliotecas, etc.) como una capa del servicio, y administrarlo y compartirlo fácilmente a través de múltiples funciones.
t. El servicio debe ser compatible de forma nativa con Java, PowerShell, Node.js, C# y Python.
u. El servicio debe proporcionar una API de tiempo de ejecución que permita utilizar cualquier lenguaje de programación adicional para crear sus funciones.
v. El servicio debe ofrecer monitoreo y creación de registros integrados a través de una herramienta específica del PSN para este propósito.
w. El servicio debe tener la capacidad de cómputo distribuida en varias ubicaciones para ayudar a proteger el código frente a fallos en equipos individuales o fallos en las instalaciones del centro de datos.
x. El servicio debe poder invocar el código solo cuando resulta necesario y debe poder escalar automáticamente para atender el porcentaje de solicitudes entrantes sin que sea necesario que el usuario realice ninguna configuración adicional.
y. El servicio no debe tener un límite del número de solicitudes que el código puede gestionar.
z. El servicio debe poder iniciar tantos recursos de cómputo de dicho código como sean necesarios sin que se produzcan largos retrasos de implementación y configuración.
aa. El servicio debe contar con un estado de simultaneidad donde al estar aprovisionado se mantengan las funciones activadas y en el mayor estado de preparación para responder en milisegundos de dos dígitos.
bb. El servicio debe permitir incrementar el nivel de simultaneidad durante los periodos de alta demanda y disminuirlo o, directamente, desactivar la simultaneidad por completo, cuando la demanda decrece.
cc. El servicio debe permitir coordinar varias funciones para tareas complejas o largas mediante la creación de flujos de trabajo.
dd. El servicio debe permitir el uso de pasos secuenciales, paralelos, bifurcados o con control de errores.

ee. El servicio debe permitir ejecutar código en respuesta a eventos y administra automáticamente los recursos informáticos subyacentes.
ff. El servicio debe permitir ampliar la funcionalidad de otros productos del PSN con lógica personalizada o bien crear servicios back-end propios que funcionen con el nivel de seguridad, rendimiento y escala de la nube pública.
gg. El servicio debe permitir ejecutar código automáticamente en respuesta a varios eventos, como solicitudes HTTP a través de un API Gateway, modificaciones realizadas en objetos contenidos en carpetas en el servicio de almacenamiento; entre otros.
hh. El servicio debe estar implementado sobre infraestructura informática de alta disponibilidad donde el PSN se encarga de la administración integral de los recursos informáticos, incluido el mantenimiento del servidor y del sistema operativo, el aprovisionamiento de capacidad y el escalado automático, la implementación de parches de seguridad y código, así como la monitorización de código y los registros.
ii. El servicio debe permitir crear funciones.
jj. El servicio debe permitir cargar código.
kk. El servicio debe permitir compilar el código.
ll. El servicio debe permitir activar otros servicios ofrecidos por el PSN.
mm. El servicio debe permitir usar cualquier biblioteca de terceros e incluso las nativas.
nn. El servicio debe permitir empaquetar cualquier código (marcos, SDK, bibliotecas, etc.) como una capa del servicio, y administrarlo y compartirlo fácilmente a través de múltiples funciones.
oo. El servicio debe ser compatible de forma nativa con Java, PowerShell, Node.js, C# y Python.
pp. El servicio debe proporcionar una API de tiempo de ejecución que permita utilizar cualquier lenguaje de programación adicional para crear sus funciones.
qq. El servicio debe ofrecer monitoreo y creación de registros integrados a través de una herramienta específica del PSN para este propósito.
rr. El servicio debe tener la capacidad de cómputo distribuida en varias ubicaciones para ayudar a proteger el código frente a fallos en equipos individuales o fallos en las instalaciones del centro de datos.
ss. El servicio debe poder invocar el código solo cuando resulta necesario y debe poder escalar automáticamente para atender el porcentaje de solicitudes entrantes sin que sea necesario que el usuario realice ninguna configuración adicional.
tt. El servicio no debe tener un límite del número de solicitudes que el código puede gestionar.
uu. El servicio debe poder iniciar tantos recursos de cómputo de dicho código como sean necesarios sin que se produzcan largos retrasos de implementación y configuración.

vv. El servicio debe contar con un estado de simultaneidad donde al estar aprovisionado se mantengan las funciones activadas y en el mayor estado de preparación para responder en milisegundos de dos dígitos.
ww. El servicio debe permitir incrementar el nivel de simultaneidad durante los periodos de alta demanda y disminuirlo o, directamente, desactivar la simultaneidad por completo, cuando la demanda decrece.
xx. El servicio debe permitir coordinar varias funciones para tareas complejas o largas mediante la creación de flujos de trabajo.
yy. El servicio debe permitir el uso de pasos secuenciales, paralelos, bifurcados o con control de errores.
zz. El servicio debe permitir la integración de API con herramientas operacionales. [VC2].
aaa. El servicio debe contar con la capacidad de otorgar permisos a la función para acceder a otros recursos.
bbb. El servicio debe contar con capacidad para enrutar solicitudes a diferentes servidores de origen backend.
ccc. El servicio debe soportar el balanceo de cargas a nivel de aplicaciones. [VC4]
ddd. El servicio debe permitir administrar de forma centralizada el código y los datos que se comparten entre múltiples funciones.
eee. El servicio debe permitir asegurar la integridad del código en la implementación con firma de código.
fff. El servicio debe soportar aplicaciones anidadas.
ggg. El servicio debe permitir solicitar la personalización del encabezado para reenviar contenido desde el origen de un objeto de almacenamiento.
hhh. El servicio debe permitir ejecutar código y responder a eventos en ubicaciones de borde.
iii. El servicio debe soportar encriptación del lado del servidor.
jjj. El servicio debe contar con la capacidad de orquestación de funciones sin servidor.
kkk. El servicio debe soportar la generación de respuesta binaria para eventos de borde.
lll. El servicio debe soportar funciones con estado.
mmm. El servicio debe soportar llamadas de red remotas desde eventos de borde orientados al espectador.
nnn. El servicio debe soportar versionamiento.
ooo. El servicio debe soportar un tiempo de ejecución de funciones máximo de 15 minutos.
ppp. El servicio debe contar con una memoria de función máxima de 10,240 MB.

9.5.19. Base de Datos de Documentos del PSN

a. El servicio debe ser compatible con MongoDB.
b. El servicio debe permitir la administración de datos JSON a escala, completamente administrado e integrado con la nube.

c. El almacenamiento del servicio debe poder escalar automáticamente hasta 64 TB sin ningún impacto en la aplicación.
d. El servicio debe admitir millones de solicitudes por segundo con hasta 15 réplicas de lectura de baja latencia.
e. El servicio debe replicar seis copias de los datos en tres ubicaciones diferentes.
f. El servicio debe ser compatible con las herramientas y los controladores de MongoDB 3.6 y 4.0.
g. El servicio debe contar con capacidades de consulta geoespacial; es decir, debe permitir el almacenamiento, las consultas y la indexación de datos geoespaciales.
h. El servicio debe contar con propiedades de las transacciones de las bases de datos pensadas para garantizar la validez de los datos a pesar de los errores, los errores de alimentación y otros contratiempos.
i. El servicio debe suministrar métricas para sus instancias de base de datos en la nube.
j. El servicio debe suministrar métricas sobre el uso de la capacidad informática, de memoria y de almacenamiento, acerca del rendimiento de las consultas, los opcounters de MongoDB y las conexiones activas.
k. El servicio debe mantener actualizada la base de datos con los parches más recientes.
l. El servicio debe permitir implementar parches y definir cuándo se aplican a través de la administración de versiones del motor de la base de datos.
m. El servicio debe contar con alto rendimiento y baja latencia para consultas de documentos.
n. El servicio debe contar con un modelo de documento JSON flexible, tipos de datos y una indexación eficiente.
o. El servicio debe permitir usar una arquitectura optimizada en memoria y de escala ajustable que permite la evaluación rápida de consultas en conjuntos de documentos de gran tamaño.
p. El servicio debe permitir escalar o reducir los recursos informáticos y de memoria mediante la creación de instancias de réplicas nuevas del tamaño que se desee o a través de la eliminación de instancias.
q. El servicio debe estar en capacidad de aumentar automáticamente el tamaño del volumen de almacenamiento a medida que se incrementen las necesidades del clúster en relación con el almacenamiento.
r. El servicio debe ser compatible con el control del acceso basado en roles (RBAC) que El servicio debe permitir cifrar las bases de datos mediante las claves creadas.
s. Las conexiones entre un cliente y el servicio deben estar cifradas en tránsito con TLS.
t. El servicio debe facilitar la recuperación ante desastres en caso de interrupciones de servicio en toda una región.
u. El servicio debe contar con capacidad de almacenamiento con recuperación automática y tolerante a errores.

v. El servicio debe permitir el restablecimiento a un momento dado.
w. El servicio debe contar con copias de seguridad automáticas, constantes y progresivas.
x. El servicio debe permitir crear instantáneas de clústeres.

9.5.20. NAT Gateway del PSN

a. El servicio debe permitir la traducción de direcciones de red (NAT).
b. El servicio debe permitir usar una puerta de enlace NAT para que las instancias de cómputo en una subred privada puedan conectarse a servicios fuera de la Nube Privada Virtual, pero los servicios externos no puedan iniciar una conexión con esas instancias de cómputo.
c. El servicio debe permitir especificar uno de los siguientes tipos de conectividad:
   - Público:
     i. Las instancias de cómputo en subredes privadas deben poder conectarse a Internet a través de una puerta de enlace NAT pública, pero no deben poder recibir conexiones entrantes no solicitadas desde Internet.
     ii. El servicio bajo este tipo de conexión debe permitir crear una puerta de enlace NAT pública en una subred pública y debe permitir asociar una dirección IP elástica con la puerta de enlace NAT en el momento de la creación.
     iii. El servicio bajo este tipo de conexión debe permitir enrutar el tráfico desde la puerta de enlace NAT a la puerta de enlace de Internet para la Nube Privada Virtual.
     iv. El servicio bajo este tipo de conexión debe permitir, como alternativa, utilizar una puerta de enlace NAT pública para conectarse a otras Nube Privada Virtual o a su red local.
     v. El servicio bajo este tipo de conexión debe permitir enrutar el tráfico desde la puerta de enlace NAT a través de una puerta de enlace de tránsito o una puerta de enlace privada virtual.
   - Privado:
     i. Las instancias en subredes privadas deben poder conectarse a otras Nubes Privadas Virtuales o a la red local a través de una puerta de enlace NAT privada.
     ii. El servicio bajo este tipo de conexión debe permitir enrutar el tráfico desde la puerta de enlace NAT a través de una puerta de enlace de tránsito o una puerta de enlace privada virtual.
     iii. El servicio bajo este tipo de conexión debe evitar asociar una dirección IP elástica con una puerta de enlace NAT privada.
     iv. El servicio bajo este tipo de conexión debe permitir asociar una puerta de enlace de Internet a una VPC con una puerta de enlace NAT privada, pero si se enruta el tráfico desde la puerta de enlace NAT privada a la puerta de enlace de Internet, la puerta de enlace de Internet descarta el tráfico.

d. La puerta de enlace NAT reemplaza la dirección IP de origen de las instancias con la dirección IP de la puerta de enlace NAT. Para una puerta de enlace NAT pública, esta es la dirección IP elástica de la puerta de enlace NAT. Para una puerta de enlace NAT privada, esta es la dirección IP privada de la puerta de enlace NAT. Al enviar tráfico de respuesta a las instancias, el dispositivo NAT vuelve a traducir las direcciones a la dirección IP de origen original.

9.5.21. Servicio de Soporte Completamente administrado para Transferencias de Archivos Directamente desde y hacia el Servicio de Almacenamiento de Objetos del PSN

a. El servicio debe ser compatible con es compatible con el protocolo seguro de transferencia de archivos (SFTP), el protocolo de transferencia de archivos a través de SSL (FTPS) y el protocolo de transferencia de archivos (FTP).
b. El servicio debe operar y administrar de manera transparente toda la computación, el almacenamiento y otra infraestructura necesaria para mantener una alta disponibilidad y rendimiento para el punto final
c. El servicio debe ser elástico.
d. El servicio debe admitir sistemas de autenticación de usuarios comunes, incluidos Microsoft Active Directory y el Protocolo ligero de acceso a directorios (LDAP). Alternativamente, también debe permitir optar por almacenar y administrar las credenciales de los usuarios directamente dentro del servicio.
e. El servicio debe permitir la conversión de archivos en objetos, un proceso que debe conservar los metadatos de archivos como metadatos de objetos.
f. El servicio debe contar con controles de acceso.
g. El servicio debe contar con opciones de autenticación.
h. El servicio debe contar con opciones para encriptación de datos.
i. El servicio debe contar con mapeo de la estructura de directorios lógicos en el almacén de datos de objetos.
j. El servicio debe contar con controles de seguridad de red.

9.5.22. Servicio Administrado de Kubernetes del PSN

a. El servicio debe permitir automatizar la implementación, el escalado y la administración de aplicaciones en contenedores.
b. El servicio debe contar con una certificación de conformidad con Kubernetes, por lo que las aplicaciones existentes que se ejecutan en el Kubernetes ascendente deben ser compatibles con el servicio.
c. El servicio debe administrar de forma automática la disponibilidad y la escalabilidad de los nodos del plano de control de Kubernetes responsables de programar contenedores, administrar la disponibilidad de las aplicaciones, almacenar datos de clústeres y otras tareas clave.

d. El servicio debe permitir ejecutar las aplicaciones de Kubernetes en servicios de la nube.
e. El servicio debe ser compatible con otros servicios de la nube.
f. El servicio debe poder ser ejecutado en diferentes ubicaciones de la nube para mejorar su disponibilidad.
g. El servicio debe administrar automáticamente la disponibilidad y la escalabilidad de los servidores API de Kubernetes y la capa de persistencia.
h. El servicio debe ejecutar el plano de control de Kubernetes en tres ubicaciones de la nube diferentes para garantizar una alta disponibilidad, al tiempo que debe detectar y sustituir automáticamente los nodos de panel de control principales que presenten errores.
i. El servicio debe proporcionar una consola integrada para clústeres de Kubernetes.
j. El servicio debe permitir instalar y mantener actualizado el software complementario.
k. El servicio debe permitir crear, actualizar, escalar y terminar nodos para el clúster con un solo comando.
l. El servicio debe ofrecer opciones para ser desplegado localmente de tal forma que sea posible ejecutar aplicaciones en contenedores que requieren latencias particularmente bajas para los sistemas en las instalaciones.
m. El servicio debe permitir crear y operar fácilmente clústeres de Kubernetes en las instalaciones, incluso en máquinas propias virtuales (VM) y servidores bare metal.
n. El servicio debe proporcionar herramientas de automatización que simplifican la creación de clústeres, la administración y las operaciones en infraestructura como bare metal, VMware vSphere y máquinas virtuales de nube.
o. El servicio debe ofrecer las herramientas y componentes adicionales que eventualmente se pueden necesitar para ejecutar Kubernetes en producción, como instalación de clústeres y administración de ciclos de vida, observabilidad, copias de seguridad de clúster y administración de políticas.
p. El servicio debe permitir usar eksctl para simplificar la administración y las operaciones del clúster, incluida la administración de nodos y complementos.
q. El servicio debe admitir nodos de trabajo de Windows y programar contenedores de Windows.
r. El servicio debe admitir la ejecución de nodos de trabajo de Windows junto con los nodos de trabajo de Linux, lo que a su vez debe facilitar el uso del mismo clúster para administrar aplicaciones en cualquier sistema operativo.

s. El servicio debe facilitar la provisión de seguridad para sus clústeres de Kubernetes, con características avanzadas e integraciones con los servicios de la nube y terceros.
t. El servicio debe ser compatible con IPv6 con el fin de que sea posible escalar las aplicaciones en contenedores en Kubernetes muy por encima de los límites de espacio de las direcciones IPv4 privadas.
u. El servicio debe configurar las redes para que los pods puedan seguir comunicándose con los puntos de conexión basados en IPv4 fuera del clúster.
v. El servicio debe permitir que ningún recurso de informática se comparta con otros clientes, con el fin de brindar un alto nivel de aislamiento para crear aplicaciones seguras y confiables.
w. El servicio debe satisfacer los requisitos de conformidad de: SOC, PCI, ISO, FedRAMP-Moderate, IRAP, C5, K-ISMS, ENS High, OSPAR, HITRUST y CSF..
x. El servicio debe permitir ejecutar el balanceador de carga de clúster estándar de Kubernetes o cualquier controlador de entrada compatible con Kubernetes.
y. El servicio debe simplificar el proceso de comprensión de los costos asociados a su uso de Kubernetes, tanto a nivel de clúster como a nivel de aplicación individual.
z. El servicio debe agregar automáticamente una etiqueta de asignación de costos de la nube a cada instancia que se une a un clúster.
aa. El servicio debe ser compatible con Kubecost para supervisar los costos desglosados por recursos de Kubernetes, incluidos pods, nodos, espacios de nombre y etiquetas.
bb. El servicio debe proporcionar visibilidad sobre operaciones de administración, incluido el historial de auditorías.
cc. El servicio debe permitir ejecuta Kubernetes ascendente y debe contar con una certificación de conformidad con Kubernetes, por lo que es posible utilizar todos los complementos y las herramientas de la comunidad de Kubernetes.
dd. Las aplicaciones que se ejecutan en el servicio deben ser completamente compatibles con las aplicaciones que se ejecutan en cualquier entorno de Kubernetes estándar, independientemente de si se ejecutan en centros de datos en las instalaciones o en nubes públicas.
ee. El servicio debe facilitar la actualización de clústeres en ejecución a la última versión de Kubernetes sin administrar el proceso de dicha actualización.
ff. El servicio debe ser totalmente compatible con las herramientas de la comunidad de Kubernetes y debe admitir complementos populares de Kubernetes. Entre ellos deben estar incluidos CoreDNS, que crea un servicio DNS para su clúster, así como la UI basada en la web de Kubernetes Dashboard y las herramientas de línea de comandos kubectl, que ayuda a acceder a su clúster y administrarlo en el servicio.

gg. El servicio debe ser compatible con instancias basadas en procesadores ARM.
hh. El servicio debe tener capacidad de recuperarse de forma automática.
ii. El servicio debe tener control granular de actualizaciones automáticas.
jj. El servicio debe soportar la encriptación de secretos.
kk. El servicio debe poder ser desplegado bajo una modalidad sin servidor.

9.5.23. Servicio de VPN Site to Site del PSN

a. El servicio debe permitir establecer conexiones seguras entre sus redes en las instalaciones de la entidad, las oficinas remotas, los dispositivos y la red global del proveedor de nube.
b. El servicio permite acceder con un túnel de protocolo seguridad de la capa de transporte (TLS) de Client VPN.
c. El servicio soporta la conexión tanto de la gateway privada virtual como de Transit Gateway.
d. El tráfico en el túnel entre los puntos de enlace debe poder encriptarse con AES128 o AES256 y utilizar protocolos Diffie-Hellman para intercambios claves.
e. El servicio debe brindar opciones de túnel personalizables, incluidos dirección IP de túnel interna, clave compartida previamente y número de sistema autónomo para protocolo de gateway fronteriza (BGP ASN).
f. Client VPN se debe poder autenticar utilizando el Active Directory o certificados.
g. Client VPN debe ofrecer autorización de la red para que sea posible definir las normas de control de acceso que limitan el acceso a redes específicas en función de los grupos de Active Directory.
h. Client VPN debe poder ofrecer acceso granular a aplicaciones específicas a los usuarios de Client VPN que utilizan los grupos de seguridad.
i. Client VPN debe poder utilizar el protocolo de túnel TLS VPN seguro para encriptar el tráfico.
j. El servicio debe permitir escoger entre clientes de OpenVPN, lo que ofrece la opción de usar el dispositivo de elección, incluidos Windows, Mac, iOS, Android y Linux.
k. Client VPN debe permitir establecer reglas de autorización que actúen como un firewall para dar acceso a redes.
l. Client VPN debe soportar SAML Authentication.
m. Client VPN debe soportar gestión de sesión y revocación para usuarios de VPN de punto a sitio.

9.5.24. Servicios de Respaldo del PSN

a. El servicio debe brindar acceso a una consola centralizada de copias de seguridad.
b. El servicio debe permitir administrar de manera centralizada políticas de copias de seguridad que cumplan con sus requisitos pertinentes y aplicarlas en recursos de la nube.

c. El servicio debe permitir definir políticas de retención de copias de seguridad automáticamente de acuerdo con los requisitos de la entidad y de conformidad normativa vinculados con el respaldo.
d. El servicio debe permitir almacenar las copias de seguridad periódicas de una manera gradual y eficiente.
e. Debe permitir los respaldos basados en snapshots.

9.5.25. Servicio de Gestión de APIs del PSN

a. Debe facilitar la creación, publicación, mantenimiento, monitoreo y securización de APIs a cualquier escala.
b. Debe permitir la definición y configuración de rutas, métodos y respuestas.
c. Debe ofrecer capacidades de rate limiting y protección contra ataques DDoS.
d. Debe permitir la integración con otros servicios y sistemas back-end.
e. Debe operar bajo un esquema de pago por uso, basado en el número de llamadas a la API y el ancho de banda de datos transferidos.

9.5.26. Servicio de Gestión de Certificados Digitales del PSN

El servicio debe crear, almacenar y renovar certificados y claves SSL/TLS X.509 que protegen sus sitios web y aplicaciones en el proveedor de nube.

9.5.27. Servicio de Transferencia de Datos en la Nube del PSN

a. El servicio debe permitir la transferencia de datos hacia y desde la infraestructura de proveedor cloud de manera eficiente y segura.
b. Debe proporcionar opciones para la transferencia de datos a través de Internet y conexiones directas dedicadas.
c. El servicio debe admitir la transferencia de datos en diferentes formatos, incluidos archivos, bases de datos y transmisiones en tiempo real.
d. Debe ofrecer opciones de compresión y cifrado para garantizar la seguridad y la eficiencia de la transferencia de datos.
e. El servicio debe ser compatible con la migración de datos hacia y desde otros proveedores de servicios en la nube y entornos locales.
f. Debe proporcionar herramientas y recursos para supervisar y gestionar la transferencia de datos, incluida la optimización de la velocidad y el rendimiento.
g. El servicio debe ser compatible con las políticas de seguridad de la organización, incluida la gestión de acceso y permisos.
h. Debe ser facturado según el volumen de datos transferidos y la velocidad de transferencia de datos.

9.5.28. Servicio de Automatización y Entrega Continua en la Nube del PSN

a. El servicio debe permitir la automatización de pipelines de entrega continua para la construcción, prueba y despliegue de aplicaciones y recursos en la nube.

b. Debe ofrecer opciones de integración con una variedad de herramientas de desarrollo, como herramientas de compilación y despliegue.
c. El servicio debe ser capaz de orquestar flujos de trabajo personalizados para la implementación de código y cambios en aplicaciones.
d. Debe proporcionar opciones para la creación de etapas de prueba y aprobación antes de la implementación en producción.
e. El servicio debe ser compatible con la instrumentación de aplicaciones y microservicios en una variedad de lenguajes de programación.
f. Debe permitir la integración con sistemas de control de versiones.
g. El servicio debe ser compatible con las políticas de seguridad de la organización, incluida la gestión de acceso y permisos.
h. Debe ser facturado según el número de pipelines y los recursos utilizados en los flujos de trabajo.

9.5.29. Servicio de Compilación y Pruebas de Código en la Nube del PSN

a. El servicio debe permitir la automatización de la construcción y prueba de código fuente desde sistemas de control de versiones de código.
b. Debe ofrecer opciones de configuración para la selección de entornos de construcción personalizados y la ejecución de pruebas automatizadas.
c. El servicio debe proporcionar información detallada sobre el proceso de construcción y resultados de pruebas, incluidos registros y notificaciones.
d. Debe ser capaz de integrarse con pipelines de entrega continua para facilitar la implementación continua.
e. El servicio debe ser compatible con una variedad de lenguajes de programación y entornos de desarrollo.
f. Debe permitir la gestión de acceso y permisos a recursos de compilación y pruebas.
g. El servicio debe ser facturado según el uso de recursos de compilación y pruebas.

9.5.30. Servicio de Repositorio de Código en la Nube del PSN

a. El servicio debe permitir la gestión y almacenamiento de repositorios de código fuente de manera segura en la nube.
b. Debe ofrecer capacidades de control de versiones y seguimiento de cambios en el código.
c. El servicio debe ser compatible con protocolos de acceso, para la colaboración en el desarrollo de software.
d. Debe proporcionar opciones de seguridad, incluida la autenticación de dos factores y la integración con servicio de autenticación y autorización de proveedor cloud, para controlar el acceso.
e. El servicio debe ser capaz de integrarse con herramientas de desarrollo y pipelines de entrega continua.
f. Debe ser compatible con las políticas de seguridad de la organización, incluida la gestión de acceso y permisos.

g. El servicio debe ser facturado según la cantidad de repositorios y el volumen de datos de código almacenados.

9.5.31. Servicio de Registro de Contenedores en la Nube del PSN

a. El servicio debe permitir la gestión y el almacenamiento de imágenes de contenedores de manera segura en la nube.
b. Debe ser compatible con contenedores Docker y permitir el uso de imágenes de contenedores en aplicaciones y flujos de trabajo de desarrollo.
c. El servicio debe proporcionar una interfaz para el almacenamiento y la recuperación de imágenes de contenedores de manera eficiente.
d. Debe ofrecer opciones de control de acceso y autenticación para garantizar la seguridad de las imágenes de contenedores almacenadas.
e. El servicio debe ser capaz de integrarse con orquestadores de contenedores Kubernetes y servicio de orquestación de contenedores propio del proveedor cloud.

10. ESPECIFICACIONES DE CAPACIDADES DE LOS SERVICIOS EN LA NUBE DEL PSN

Las especificaciones de capacidades siguientes deberán cotizarse para el consumo de Banco de la nación, a no ser que estos servicios de Nube se entreguen en su totalidad en modalidad SaaS 100% gestionada por el contratista a costo fijo, ya sea para los servicios compartidos, los componentes a demanda y para los ambientes de Producción, Certificación (QA) y Desarrollo (Dev).

Leyenda Nomenclaturas:

M = Millones MB = Megabytes GB = Gigabytes
TB = Terabytes HA = High Availability MS = milisegundos
TX Transacciones VM Máquina virtual

10.1. Servicios Compartidos

Tabla 8: Cuadro los Servicios Compartidos

Componentes del Servicio	Características	Unidad de medida	Cantidad Mensual Año 1	Cantidad Mensual Año 2	Cantidad Mensual Año 3
Servicio de NAT Horas	Cantidad de gateways	Unidad	3	3	3
	Horas de servicio	Horas	730x3 = 2,190	730x3 = 2,190	730x3 = 2,190
	Data Procesada	GB	98	6,870	7,560
Conexión VPN Site to Site	Cantidad de VPN	unidad	1	1	1
	Horas de servicio	Horas	730	730	730
Conexión Cliente VPN	Número de subnets asociadas	unidad	2	2	2

	Número de clientes activos	unidad por día	15	15	15
	Duración promedio por conexión	Horas	12	12	12
	Días laborables por mes	Días	22	22	22
Conector de redes en múltiples zonas	Cantidad de attachments	unidad	3	3	3
	Horas de servicio	Horas	730x3 = 2,190	730x3 = 2,190	730x3 = 2,190
	Datos procesados	GB	98	6,870	7,560
Servicio de transferencia de datos	Transferencia de datos salientes (GB)	GB	98	6,870	7,560
Kit de desarrollo de software en la nube	Número de instancias	unidad	5	5	5
	Numero de despliegues	Horas	730x5 = 3,650	730x5 = 3,650	730x5 = 3,650
Servicio de entrega continua	Pipelines	unidad	100	100	100
Repositorio de paquetes de software	Número de artefactos almacenados	GB	120	240	360
	Solicitudes de API	unidad	5,000,000	5,000,000	5,000,000
	Data Procesada	GB	120	240	360
Servicio de construcción e integración continua con Sistema operativo Linux. Recurso de cómputo con las siguientes características: 8 vCPU y 16 GB Memoria	Número de compilaciones	unidad	2,000	2,000	2,000
	Duración de compilación	minutos	2,000x5 = 10,000	2,000x5 = 10,000	2,000x5 = 10,000
Registro de contenedores	Cantidad de datos almacenados (GB)	GB	400	800	1200
	Tráfico de salida	GB	400	800	1200
Servicio de autenticación Web/móvil	Usuarios activos por mes	Unidad	100	3,600,000	5,200,000
Servicio de logs de la consola en nube	Eventos registrados de escritura	1M	10	10	10
	Eventos registrados de lectura	1M	10	10	10

10.2. Ambiente de Producción

Tabla 9: Cuadro del Ambiente de Producción

Componentes del Servicio	Características	Unidad de medida	Cantidad Mensual	Cantidad Mensual	Cantidad Mensual

			Año 1	Año 2	Año 3
Servicio de base de datos relacional compatible con PostgreSQL en alta disponibilidad (Primario/Respaldo) en multizona Cada característica puede consumirse de manera independiente	4 vCPU y 16 GB RAM	Horas	730	0	0
	16 vCPU y 64 GB RAM	Horas	0	730	730
	SSD	GB	1	200	500
	Storage para respaldo	GB	2	220	550
Servicio de base de datos de documentos compatible con (mongoDB) Cada característica puede consumirse de manera independiente 2 Instancias, una por Zona de disponibilidad	2 vCPU y 16 GB RAM	Horas	730x2 = 1,460	0	0
	4 vCPU y 32 GB RAM	Horas	0	730x2 = 1,460	730x2 = 1,460
	SSD	GB	10	500	1000
	Storage para respaldo	GB	11	550	1100
	Peticiones I/O	1M I/O	3.4	240	264
Servicio de administración y despliegue de APIs	Solicitudes de API REST	1M de Solicitudes	3.4	240	264
Balanceador de carga de red	Horas de Ejecución	Horas	730	730	730
	Data procesada en GB	GB procesados	98	6,870	7,560
	Conexión TCP por minuto	Unidad por minuto	78	5,480	6,030
Servicio de contenedores basado en Kubernetes	Uso de servicio	Horas	730	730	730
Servicio de máquinas virtuales de cómputo para kubernetes con Sistema operativo Linux	4 vCPU y 8 GB RAM	Horas	730X8 = 5,840	730X8 = 5,840	730X8 = 5,840
	SSD	GB	50x8=400	50x8=400	50x8=400
	Storage para respaldo	GB	55x8=440	55x8=440	55x8=440
Servicio de CDN	Número de solicitudes (HTTPS)	1 solicitud	340,000	24,000,000	26,400,000
	Transferencia de	GB	98	6,870	7560

	datos salientes (GB)				
Servicio de gestión de claves criptográficas	Llaves	1 unidad	50	50	50
	Solicitudes de cifrado y descifrado	Peticiones	6,800,000	480,000,000	528,000,000
Servicio de almacenamiento de secretos	Secretos almacenados	1 unidad	100	100	100
	Actividad del servicio de secretos	Horas	730	730	730
	Solicitudes	1 unidad	340,000	24,000,000	26,400,000
Servicio de almacenamiento de objetos	Almacenamiento estándar	GB	50	50	50
	Solicitudes a la API de objetos GET	1 Petición	340,000	24,000,000	26,400,000
	Solicitudes a la API de objetos PUT, COPY, POST o LIST	1 Petición	34,000	2,400,000	2,640,000
Servicio de monitoreo y observabilidad	Métricas Personalizadas	1 unidad	100	100	100
	Número de peticiones	1 unidad	340,000	24,000,000	26,400,000
	Almacenamiento de Logs	GB	10	100	100
	GB analizados de Logs	GB	5	5	5
	Alarmas	1 unidad	50	50	50
	Dashboards	1 unidad	5	5	5
	Métricas para Contenedores	1M	3.4	240	264
SFTP	Servicio activo	Horas	730	730	730
	Carga de datos	GB	30	30	30
	Descarga de datos	GB	30	30	30
Servicio de ejecución de Funciones sin servidor	Número de peticiones	1 unidad	340,000	24,000,000	26,400,000
	Duración promedio de petición	1 ms	100	100	100
	Memoria utilizada	Mb	512	512	512

10.3. Ambiente de Certificación (QA)

Tabla 10: Cuadro del Ambiente de Certificación (QA)

Componentes del Servicio	Características	Unidad de medida	Cantidad Mensual Año 1	Cantidad Mensual Año 2	Cantidad Mensual Año 3
Servicio de base de datos relacional compatible con PostgreSQL en	4 vCPU y 16 GB RAM	Horas	730	730	730
	SSD	GB	1	20	50

alta disponibilidad (Primario/Respaldo) en multizona	Storage para respaldo	GB	2	22	55
Servicio de base de datos de documentos compatible con (mongoDB) Cada característica puede consumirse de manera independiente 2 Instancias, una por Zona de disponibilidad	2 vCPU y 16 GB RAM	Horas	730x2 = 1,460	730x2 = 1,460	730x2 = 1,460
	SSD	GB	10	50	100
	Storage para respaldo	GB	11	55	110
	Peticiones I/O	1M	1	20	27
Servicio de administración y despliegue de APIs	Solicitudes de API REST	1M	1	20	27
Balanceador de carga de de aplicación	Horas de Ejecución	Horas	730	730	730
	Data procesada en GB	GB procesados	10	548	603
Servicio de contenedores basado en Kubernetes	Uso de servicio	Horas	730	730	730
Servicio de máquinas virtuales de cómputo con Sistema operativo Linux	4 vCPU y 8 GB RAM	Horas	4x730 = 2,920	4x730 = 2,920	4x730 = 2,920
	SSD	GB	50x4 = 200	50x4 = 200	50x4 = 200
	Storage para respaldo	GB	55x4 = 220	55x4 = 220	55x4 = 220
Servicio de CDN	Número de solicitudes (HTTPS)	Peticiones	34,000	2,400,000	2,640,000
	Transferencia de datos salientes	GB	10	580	780
Servicio de gestión de claves criptográficas	Llaves	Cantidad	50	50	50
	Solicitudes de cifrado y descifrado	Peticiones	680,000	48,000,000	52,800,000
Servicio de almacenamiento de secretos	Secretos almacenados	1 unidad	100	100	100
	Actividad del servicio de secretos	Horas	730	730	730
	Solicitudes	1 unidad	34,000	2,400,000	2,640,000
Servicio de almacenamiento de objetos	Almacenamiento estándar	GB	50	50	50
	Solicitudes a la	1 Petición	34,000	2,400,000	2,640,000

	API de objetos GET				
	Solicitudes a la API de objetos PUT, COPY, POST o LIST	1 Petición	3,400	240,000	264,000
Servicio de monitoreo y observabilidad	Métricas Personalizadas	1 unidad	10	10	10
	Número de peticiones	1 unidad	3,400	24,000	26,400
	Almacenamiento de Logs	GB	5	5	5
	GB analizados de Logs	GB	5	5	5
	Alarmas	Cantidad	5	5	5
	Dashboards	Cantidad	5	5	5
	Métricas para Contenedores	1M	1	20	27
SFTP	Servicio activo	Horas	730	730	730
	Carga de datos	GB	10	10	10
	Descarga de datos	GB	10	10	10
Servicio de ejecución de Funciones sin servidor	Número de peticiones	1 unidad	34,000	2,400,000	2,640,000
	Duración promedio de petición	1 ms	100	100	100
	Memoria utilizada	Mb	512	512	512

10.4. Ambiente Desarrollo (DEV)

Tabla 11: Cuadro del Ambiente de Desarrollo (DEV)

Componentes del Servicio	Características	Unidad de medida	Cantidad Mensual Año 1	Cantidad Mensual Año 2	Cantidad Mensual Año 3
Servicio de base de datos relacional compatible con PostgreSQL	4 vCPU y 16 GB RAM	Horas	730	730	730
	SSD	GB	10	20	30
	Storage para respaldo	GB	11	22	33
Servicio de base de datos de documentos compatible con (mongoDB)	2 vCPU y 16 GB RAM	Horas	730	730	730
	SSD	GB	10	20	30
	Storage para respaldo	GB	11	22	33
	Peticiones I/O	1M	1	1	1
Servicio de administración y despliegue de APIs	Solicitudes de API REST	1M	10	10	10
Balanceador de carga de aplicación	Horas de Ejecución	Horas	730	730	730
	Data procesada GB	GB	10	10	10

		procesados			
Servicio de contenedores basado en Kubernetes	Uso de servicio	Horas	730	730	730
Servicio de máquinas virtuales de cómputo con Sistema operativo Linux	4 vCPU y 8 GB RAM	Horas	2x730 = 1,460	2x730 = 1,460	2x730 = 1,460
	SSD	GB	50x2	50x2	50x2
	Storage para respaldo	GB	55x2	55x2	55x2
Servicio de CDN	Número de solicitudes (HTTPS)	Peticiones	34,000	34,000	34,000
	Transferencia de datos salientes (GB)	GB	10	10	10
Servicio de gestión de claves criptográficas	Llaves	Cantidad	50	50	50
	Solicitudes de cifrado y descifrado	Peticiones	680,000	680,000	680,000
Servicio de almacenamiento de secretos	Secretos almacenados	1 unidad	100	100	100
	Actividad del servicio de secretos	Horas	730	730	730
	Solicitudes	1 unidad	34,000	34,000	34,000
Servicio de almacenamiento de objetos	Almacenamiento estándar	GB	50	50	50
	Solicitudes a la API de objetos GET	1 Petición	34,000	34,000	34,000
	Solicitudes a la API de objetos PUT, COPY, POST o LIST	1 Petición	3,400	3,400	3,400
Servicio de monitoreo y observabilidad	Métricas Personalizadas	Cantidad	10	10	10
	Número de peticiones	1 unidad	3,400	3,400	3,400
	Almacenamiento de Logs	GB	5	5	5
	GB analizados de Logs	GB	5	5	5
	Alarmas	Cantidad	5	5	5
	Dashboards	Cantidad	5	5	5
	Métricas para Contenedores	1M	1	1	1
SFTP	Servicio activo	Horas	730	730	730
	Carga de datos	GB	10	10	10
	Descarga de datos	GB	10	10	10
Servicio de ejecución de Funciones sin servidor	Número de peticiones	1 unidad	34,000	34,000	34,000
	Duración promedio de petición	1 ms	100	100	100
	Memoria utilizada	Mb	512	512	512

10.5. Componentes a Demanda

Tabla 12: Cuadro de los Componentes a Demanda

Componentes del Servicio	Características	Unidad de medida	Cantidad Mensual
Servicio de base de datos relacional (HA)	8 vCPU	Horas	730x2 = 1,460
	128 GB RAM		
	16 vCPU	Horas	730x2 = 1,460
	128 GB RAM		
	32 vCPU	Horas	730x2 = 1,460
	256 GB RAM		
Servicio de base de datos de documentos	4 vCPU	Horas	730x2 = 1,460
	32 GB Memoria RAM		
	8 vCPU	Horas	730x2 = 1,460
	64 GB Memoria RAM		
	16 vCPU	Horas	730x2 = 1,460
	128 GB Memoria RAM		
Servicio de máquinas virtuales de cómputo para kubernetes con Sistema operativo Linux	4 vCPU	Horas	730x8 = 5,840
	16GB RAM		
	8 vCPU	Horas	730x8 = 5,840
	16GB RAM		
Direct Connet hosteado	Transferencia salida de PSN	GB	10,240
	Ancho de banda	GB	10
	Tiempo	Horas	730
	Puertos	unidad	2

*Este servicio podrá ser activado durante el plazo del contrato a solicitud del Banco de la Nación y estará sujeto a modificaciones de acuerdo los requerimientos del Banco de la Nación.

11. PRESTACIÓN DEL SERVICIO DE SEGURIDAD A CONTRATAR

11.1. Implementación de los Servicios de Seguridad

Con el propósito de fortalecer nuestra postura de seguridad informática, se establece como requisito esencial en estos términos de referencia la contratación de servicios de seguridad de terceros. El CONTRATISTA seleccionado deberá implementar soluciones de seguridad robustas y actualizadas, abarcando aspectos como la monitorización proactiva, detección y respuesta ante amenazas, así como la implementación de medidas de prevención. Se espera que los servicios contratados cumplan con los estándares de seguridad más recientes y se integren de manera eficiente con nuestra infraestructura existente. La capacitación de nuestro personal en las mejores prácticas de seguridad y la asesoría continua para la mejora de nuestros protocolos son elementos clave que buscamos incluir en este contrato.

El CONTRATISTA deberá implementar y asegurar los siguientes servicios de seguridad descritos para la Infraestructura pública o Nube pública donde se alojará la solución:

11.2. Consola SaaS de Seguridad para los Servicios WAF, Ataques Volumétricos de Denegación de Servicio y Servicio de Seguridad de APIs

La solución SaaS debe realizar la ejecución de políticas de seguridad sobre aplicaciones y APIs, dentro de sus POPs y múltiples nubes. También teniendo la posibilidad de aplicar dichas políticas en premisas del cliente.

La solución SaaS debe soportar una arquitectura completamente SaaS, donde la manera de consumo de los servicios será completamente dentro de la nube del fabricante, incluyendo todos los puntos de presencia distribuidos de manera global.

a) Administración:

La solución SaaS deberá proporcionar una consola para administración centralizada de las configuraciones de Red y seguridad, así como para acceso a troubleshooting y visibilidad de disponibilidad de servicios, permite la administración realizando clickops, API requests, terraform o CI/CD.

La solución SaaS deberá ser API first, permite realizar todas las configuraciones a través de las APIs, así como la petición de información de los dashboards. Se deberá permitir la creación de credenciales por usuario, API token, Certificate, así como la creación de usuarios Api con control de acceso basado en roles.

La solución SaaS deberá soportar la creación de múltiples usuarios, así como roles de acceso como read only, SecOps, DevOps, NetOps, SuperUser, Billing User entre otros.

La plataforma utiliza RBAC para el control del acceso de usuario, permitiendo la delimitación de las APIs/recursos que se pueden

visualizar, administrar, escribir dentro de un tenant o namespace.
La solución SaaS deberá ofrecer al usuario la posibilidad de administrar sus servicios dentro de una consola unificada permitiendo la colaboración de distintos equipos.

b) Visibilidad:

La solución SaaS deberá proporcionar integración con herramientas de loging como Splunk, datadog y slack.
La solución SaaS deberá proporcionar visibilidad para: Salud de la aplicación, alertas activas, Servidores de Origen, Latencia de fin a fin, Visitantes únicos, Tipo de dispositivo, Peticiones (Request Rate, Total Request, Error rate, total errors, drop rate, drop count) Troughput, tipo de dispositivo, ASN, TLS Fingerprint, TLS Ciphers y protocolos, códigos de error de http, localización de clientes, Top URL utilizada.
La solución SaaS deberá proporcionar visibilidad sobre los eventos de seguridad por cada aplicación, top ten de las firmas con más hits, eventos localizados geográficamente, eventos de WAF y políticas afectadas recientemente, tipos de ataques, sCore de usuarios maliciosos, eventos de seguridad de DDoS y deberá proporcionar filtros para búsqueda de support ID.
La solución SaaS deberá proporcionar visibilidad sobre los cambios realizados por los usuarios a las configuraciones durante el pasado mes
La solución SaaS deberá proporcionar visibilidad sobre: disponibilidad de servicios, incluyendo salud, servicios activos, latencia, errores http, request rate, troughput.
La plataforma SaaS deberá contar con 99.99% de disponibilidad.

c) Seguridad

La solución SaaS debe contar con motor de Machine Learning y firmas para la detección de ataques a nivel de capa de aplicación con detección de Owasp top 10, así como los últimos ataques conocidos con actualización automática en valores de firmas, así como la utilización de una base de datos asistida de campañas de amenazas para detección de ataques específicos alrededor del mundo y realizar la categorización de firmas por high, medium y low accuracy.
La solución SaaS debe utilizar su motor de WAF para realizar un perfilamiento de usuarios, utilizando: la cantidad de firmas identificadas, cantidad de accesos prohibidos, errores de login, tasa de errores.
La solución SaaS debe utilizar un modelo probabilístico de machine learning para el perfilamiento del tráfico dentro del WAF con lo cual se pueda realizar la supresión de falsos positivos a firmas dentro de cada balanceador de carga.
La solución SaaS debe detectar y mitigar automáticamente los ataques volumétricos de denegación de servicio sin límite de eventos y ancho de banda mínimo de capacidad de mitigación de 13Tbps.
La solución SaaS debe permitir el bloqueo de clientes basado en

comportamiento y la utilización de políticas de retos de identificación con JavaScript y Captcha.
La solución SaaS debe utilizar una lista dinámica de reputación de IP que bloquee de manera automatizada clientes maliciosos. Incluyendo categorías como SPAM, BOTNETS, PHISHING, Tor network, etc.
La solución SaaS debe permitir el bloqueo de clientes basándose en comportamiento, ASN SubnetIP, IP y país.
"La solución SaaS debe permitir la configuración de Cifrados de acuerdo con el perfil alto, medio o bajo, así como la creación de políticas personalizadas para utilización de ciphers y protocolos específicos por aplicación. High:
TLS 1.2 y 1.3 TLS_AES_128_GCM_SHA256
TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1305_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 Medium:
TLS 1.0 1.3 TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA Low: TLS 1.0 TLS 1.3
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_256_GCM_SHA384"
La solución SaaS debe permitir la configuración de certificados públicos firmados de manera automática y controlados de manera automática a través de alguna delegación de dominio o validación de registros de DNS.
La solución SaaS debe permitir la configuración de reescrituras, así como tratamiento sobre las peticiones HTTP a las aplicaciones y respuestas personalizadas de distintos códigos de HTTP.
La solución SaaS deberá permitir la configuración de monitores de salud y orígenes ilimitados con métodos de balanceo como: RoundRobin, Least Active Request, random, persistencia Origen IP, persistencia basada en cookie, Ring hash policy. Así como crear pesos sobre los orígenes que se deseen y asignar orígenes primarios.
La solución SaaS deberá contar con análisis de comportamiento, el cual deberá visualizarse en un plano de control centralizado, utiliza métricas y logs, recolectados de los proxies para crear el modelo. Este modelo deberá distribuirse a todos los puntos de presencia de la solución SaaS.
Los análisis de comportamiento incluyen: Detección de anomalías por petición, utilizando métricas como tamaño de la petición, tamaño de la

respuesta, latencia. Lógica de Negocio, el sistema utiliza los logs de peticiones, por cliente por servidor y el host virtual para aprender: elementos dinámicos, probabilidad de función, tiempos y anomalías analiza esto utilizando redes neuronales.
La solución SaaS debe permitir el uso de un mismo certificado a través de distintos load balancer.
La solución SaaS debe permitir que el cliente subir sus Swagger files para cada versión de la API, controlando el modo de consumo de los endpoints por frecuencia, método http, todo lo que no se encuentra dentro de la definición de Open API (swagger file) o explícitamente permitido será bloqueado. permite la creación de políticas de seguridad, para excepciones donde se permite el acceso a usuarios específicos dentro de API end Ponts o grupos de API.
La solución SaaS debe permitir subir distintos archivos Swagger, dependiendo de la versión de la API a proteger, y añadir la definición en distintos segmentos dentro del balanceador de carga.
La solución SaaS debe controlar la cantidad de peticiones por minuto o por segundo que un usuario identificado (ver User Identifier) puede realizar sobre todo el sitio o sobre endpoints específicos.
La solución SaaS debe controlar los subdominios permitidos en las peticiones cruzadas dentro de un balanceador de carga.
La solución SaaS debe controlar la información a visualizar dentro de las respuestas del servidor, permitiendo sustituir respuestas con para el enmascaramiento de información sensible.
La solución SaaS debe contar con un sistema de protección multifase a las aplicaciones Web, contra Formjacking, Magecart-style, y otros ataques de JS. La protección multifase incluye detección, alertamiento y mitigación.
La solución SaaS debe permitir identificar usuarios bajo los siguientes parámetros: ClientIP, TLSFingerprint, Cookie, HTTP Header, Client ASN, Client City, Client Región, Query Parameter Key.
La solución SaaS debe utilizar el mismo motor de WAF en todos sus tipos de arquitectura, SaaS e Híbrido, permitiendo la extensión de las políticas a diferentes ambientes dentro del tenant, donde, la protección puede estar en sitios públicos o privados.
La solución SaaS puede utilizar MTLS para comunicación hacia los clientes y hacia los servidores.
La solución SaaS debe realizar el aseguramiento de APIs, estableciendo atributos como, SameSite, HTTP Only y Secure, en las respuestas de cookies. Permite habilitar Cookie Tampering Protection, para evitar la modificación de la cookie de autenticación.
La solución SaaS Saas debe permitir la definición del API endpoint, así como los métodos de http que pueden consumirlo, el tamaño total del query, la profundidad máxima del request, la cantidad máxima de request realizados en batch, validación de los queries, realizando introspección,

de los recursos, disponibles en el esquema actual.
La solución SaaS debe realizar la redirección de peticiones a distintos grupos de orígenes dependiendo de: prefijo de uri, http header, cookie, método http. Aplicando reglas de WAF por cada ruta, así como reglas de seguridad específicas.
La solución SaaS debe realizar el seguimiento del comportamiento de los usuarios permitiendo la categorización de estos en 3 segmentos, low, medium, high dependiendo del puntaje por los eventos de seguridad de un usuario, XC puede realizar una mitigación automática de estos usuarios bloqueándolos por un periodo, o mandando un challenge de JS o Captcha.
La solución SaaS debe permitir crear un mensaje de respuesta personalizado por cada respuesta de código de htttp de error entregada al usuario.
La solución SaaS debe permitir limitar el tamaño de los headers en el request de los usuarios.
La solución SaaS debe permitir eliminar o añadir nuevos headers en las respuestas o peticiones entre el cliente y servidor
La solución SaaS debe permitir el control de acceso desde bloques de IP de países, por lo que se pueden manejar reglas de allow o deny desde países en específico, por ejemplo, permitir acceso solo de un país, bloqueando el resto.
La solución SaaS debe permitir la creación de reglas de L3, L7 para permitir o negar el acceso a recursos, así como el manejo de los diferentes motores de seguridad para la creación de excepciones.
La solución SaaS deberá contar con Threat Capaigns basado en ataques utilizados "In-the-wild" utiliza información contextual de ataques reales utilizados alrededor del mundo para la creación de firmas de WAF en tiempo real.
En caso de que el proveedor ofrezca un servicio SaaS integral, gestionando completamente los servicios de seguridad (incluyendo WAF), el monitoreo de la disponibilidad y resolución de problemas se presentará en un Acuerdo de Nivel de Servicio (SLA) con reportes mensuales, y adicionales a solicitud, sobre el estado del servicio. Al asumir el proveedor la responsabilidad total de la administración de la seguridad, los puntos mencionados en el apartado 11.2 podrían no ser considerados. Esta modalidad solo será aceptada en la implementación tipo SaaS integral en la nube.

11.3. Servicio de Protección de APIs

La solución SaaS debe contar con la funcionalidad de APIs Discovery, la cual debe permitir aprender de los endpoints, incluyendo petición y respuesta, detectando información sensible. Además, provee la vista de API endpoints en inventario, shadow y descubiertas. La solución SaaS genera un Probability Distribution Function (PDF) para las métricas relacionadas a cada endpoint es

generada. el análisis es generado de forma periódica, y los PDFs son actualizados de acuerdo con eso.

La solución SaaS tener la capacidad de detectar información sensible como parte del API Discovery, permitiendo identificar y localizar información sensible, en las peticiones y respuestas de las API endpoints. Identifica PII, como, números de tarjeta de crédito, numero de seguridad social. Una vez detectado, la solución SaaS deberá especificar el campo donde la información está localizada.

EL API endpoint es la combinación entre URL y método http. La solución SaaS debe permitir habilitar API endpoint Learning. La cual debe generar los siguientes beneficios: Descubrimiento dinámico de las APIs, determinar cuáles endpoints deberían ser utilizados y permitir únicamente estos API endpoints, obtener información de la utilización, como tamaño de las peticiones y frecuencia. La información obtenida nos dará las siguientes métricas: tamaño de la petición/respuesta, latencia con datos y latencia sin datos, frecuencia de peticiones, frecuencia de errores, troughput de las respuestas.

La solución SaaS debe aprender la estructura del esquema, analizando las peticiones y respuestas para cada API. Lo siguiente es aprendido de cada campo: Regex, PII, permite la descarga del swagger file aprendido.

La solución SaaS debe contener sensores integrados para la detección de tipos de autenticación, y localización en las llamadas API. Una vez detectados, estas son asociadas con un endpoint. Y se muestra un estado de autenticación.

La solución SaaS debe descubrir los headers, payload y firma de JWTs así como la identificación de campos útiles para el cliente, permite la identificación de datos sensibles en los payloads de JWT así como la definición del sCore de riesgo.

La solución SaaS debe utilizar su motor de WAF para realizar un perfilamiento de usuarios, utilizando: la cantidad de firmas identificadas, cantidad de accesos prohibidos, errores de login, tasa de errores

La solución SaaS debe realizar el seguimiento del comportamiento de los usuarios permitiendo la categorización de estos en 3 segmentos, low, medium, high dependiendo del puntaje por los eventos de seguridad de un usuario, XC puede realizar una mitigación automática de estos usuarios bloqueándolos por un periodo, o mandando un challenge de JS o Captcha.

La solución SaaS debe controlar la cantidad de peticiones por minuto o por segundo que un usuario identificado puede realizar sobre todo el sitio o sobre endpoints específicos.

La solución SaaS debe estar en capacidad de usar todos los elementos descubiertos como: Información sensible, superficie de ataque y vulnerabilidades en los endpoints de API para priorizar los esfuerzos de mitigación para el equipo de seguridad.

En caso de que el proveedor ofrezca un servicio SaaS integral, gestionando completamente los servicios de seguridad (incluyendo la seguridad de las APIs), deberá entregar informes mensuales sobre seguridad e incidencias, así como informes adicionales a demanda. Al asumir el proveedor la

responsabilidad total de la administración de la seguridad y contar con un equipo de respuesta ante incidentes 24x7, los puntos mencionados en el apartado 11.3 no serán considerados. Esta modalidad solo será aceptada en la implementación SaaS integral en la nube.

11.4. Servicio de Detección Avanzada para Ataques de Bots Automatizados

El servicio de detección de Bots será implementado y facturado a solicitud del Banco en base a las necesidades que este pueda tener y se tendrá considerado dentro de estos términos de referencia y presupuesto. Para esto el postor deberá de incluir la implementación de este en la arquitectura, así como los costos relacionados al uso de este.

La solución SaaS no debe requerir que el Banco brinde ningún tipo de información confidencial como número de tarjeta o nombre de usuario para poder realizar el bloqueo en la fase de protección contra cualquier tipo de BOT.

La solución SaaS debe ejecutarse de forma independiente a la solución SaaS tecnológica de WAF que cuenta el Banco.

La solución SaaS debe indicar el número máximo llamadas HTTP/S que soportará o gestionará por día.

La solución SaaS debe de ayudar a garantizar que las aplicaciones de los canales digitales del Banco de la Nación estén protegidas contra ataques automatizados, así como a proteger aplicaciones y cuentas contra intentos de fraude automatizados.

La solución SaaS debe incluir sugerencias y consejos correctivos para todas las aplicaciones involucradas en los resultados confirmados. Proteger puntos finales específicos de aplicaciones en línea, incluidos sitios web, aplicaciones móviles y API's. Ofrecer un modelo de seguridad como servicio completamente administrado para ayudar al Banco de la Nación con la automatización de las capacidades de administración y reducir costo operativo para administrar la automatización.

11.5. Requerimientos de Detección y Mitigación

La solución SaaS debe proporcionar las siguientes características:

- Proporcionar un motor de decisiones en tiempo real para detectar y mitigar las transacciones automatizadas dirigidas a las aplicaciones protegidas del Banco.
- Recopilar señales de interacción (telemetría) del navegador/dispositivo y del usuario a través de JavaScript en aplicaciones web y un SDK en aplicaciones móviles nativas de IOS y Android para mejorar la capacidad del motor de ejecución en tiempo real para detectar ataques.
- La solución SaaS debe soportar la ofuscación de la telemetría recolectada en los clientes para no permitir la ingeniería inversa.
- Realizar la detección de bots en tiempo real, mediante pruebas con inyección de Javascript para aplicaciones web, así como SDK para

aplicaciones móviles, APIs y otras métricas que permitan su tratamiento y protección de las APP.

- La solución SaaS debe diferenciar entre solicitudes legítimas realizadas por usuarios humanos y solicitudes realizadas por bots, web scraping y ataques automatizados, en aplicativos web o móvil en tiempo real.
- La solución SaaS debe determinar si la transacción está siendo ejecutada por un humano o componente automatizado, en aplicativos web o móvil en tiempo real.1) A través de la función de las señales de la red, 2) la biometría del comportamiento, 3) la identidad del dispositivo y el análisis del cliente.
- Categorizar los robots en función de sus acciones e impacto en la infraestructura del servicio.
- Permitir la aplicación de acciones de seguridad para robots, permitiendo al menos las siguientes opciones:
    a. Permitir el acceso
    b. Bloquear el acceso y devolver el código de error HTTP 403 (acceso denegado)
    c. Bloquear acceso y regresar con mensaje personalizado
    d. Retrasar la respuesta a las solicitudes de forma personalizada
    e. Mantener la conexión abierta sin respuesta
    f. Redirigir acceso a contenido alternativo (otro servidor)
- Debe gestionar activamente las amenazas de bots, manejando su tratamiento en base a comportamiento, origen, posibilitando la creación de controles y reglas estándar y personalizadas, que garanticen el tratamiento de al menos los siguientes ataques:
    a. Límite de tarifa (rate limit) para consumos identificados como anormales
    b. Ataques DoS y DDoS
    c. Ataques de relleno de credenciales
    d. Ataques de fuerza bruta (ataque de fuerza bruta y descifrado de contraseñas)
    e. Extracción de datos (Web Scraping)
    f. Robo de identidad (Adquisición de cuenta)
    g. Debe proteger aplicaciones WEB, APIs y aplicaciones móviles nativas.
- Para aplicaciones WEB debe tener detección de anomalías de comportamiento para páginas transaccionales importantes, protegiéndolas como puntos finales de recursos API.
- Para las aplicaciones móviles nativas (Android e IOS), debe recopilar datos que incluyen, entre otros:
    a. Características del dispositivo (sistema operativo, resolución SaaS de pantalla, brillo de pantalla, hardware)
    b. Eventos táctiles de pantalla
    c. Versionado de aplicaciones
    d. Información de la batería (temperatura, capacidad, tecnología)

e. Datos del sensor físico (altitud, orientación, giroscopio)
f. Datos del acelerómetro, etc. durante la interacción del usuario.
g. Marca de tiempo de la época
h. Datos de WebView
i. Detección de emulador
j. Detección de dispositivos rooteados
k. Datos de comportamiento (tecla arriba, tecla abajo, clic del mouse, evento del mouse capturado, movimiento de alta velocidad entre dos puntos, pausa larga, transición de evento sin mouse a evento con mouse)

- Detecta diferentes actividades de bots en capas para proteger el ambiente web o móvil.
- Utilizar modelos que permitan el aprendizaje automático para la mejora del servicio.
- Incluir análisis del comportamiento del usuario, huellas dactilares del navegador, detección automática del navegador, detección de anomalías HTTP y alta tasa de solicitud de servicios.
- Debe tener una única interfaz de acceso con informes de tendencias generales, históricas y en tiempo real y análisis detallado de bots individuales u otros segmentos de tráfico de bots.
- El servicio debe detectar al menos los siguientes tipos de bots maliciosos:
  a. Bots de Tipo Scripts
  b. Bots avanzados que utilices headless browsers
  c. Bots que utilicen Browser completo y que emulen comportamiento humano programático
  d. Bots avanzados que emulen comportamiento humano y que modifiquen aleatoriamente su dirección IP y/o identificador de dispositivo.
- El servicio debe cubrir al menos los siguientes tipos de ataques automatizados:
  a. Account take over
  b. Web Scrapping
  c. Appplication DDoS
  d. Skewed Analytics
  e. Form Spam
  f. API Abuse
  g. Digital Fraud
- La solución SaaS debe estar basada en tecnología que permita detectar la intención del tráfico y el comportamiento de los usuarios con el fin de mitigar las amenazas automatizadas avanzadas de forma precisa sin impactar el tráfico legítimo de los clientes.
- El servicio debe contar con al menos los siguientes mecanismos de detección y mitigación:

a. Inteligencia de bots maliciosos compartida entre usuarios del servicio.
b. Reputación de IP para seguimiento de tráfico que provenga de proxys.
c. Machine Learning semi-supervisado para identificar patrones de bots emergentes
d. Análisis de comportamiento de los usuarios para detección de anomalías
e. Test de turing reversos y dinámicos para descubrir la identidad del bot
f. Creación del fingerprinting único por cada conexión

- El servicio debe contar, con al menos, los siguientes métodos de mitigación para bots maliciosos:
  a. Bloqueo de solicitudes
  b. Bloqueo basado en la tasa de tráfico.
  c. Alimentar a la bot con datos falsos
- El servicio debe identificar y clasificar los bots legítimos.
- El servicio debe permitir la configuración de al menos las siguientes acciones específicas sobre los bots legítimos:
  a. Bloqueo de las solicitudes
  b. Alimentar a la bot con datos falsos
- La solución SaaS debe contar con cientos de señales para detectar el comportamiento automatizado mediante la integración de la red, el navegador / dispositivo y la interacción del usuario.
- Asegurar las señales protegidas de la visibilidad y la manipulación por parte de un atacante.
- Estar diseñado para adaptarse y mantener una eficacia total incluso cuando los atacantes evolucionan e intentan reorganizarse.
- Aprovechar la inteligencia de amenazas en una red global de clientes y utilizar la inteligencia artificial (IA) para crear nuevas contramedidas y detener a los atacantes más sofisticados.
- Clasificar el tráfico automatizado en "listas permitidas" o "listas bloqueadas", para evitar el bloqueo de una buena automatización.
- La solución SaaS debe ser capaz de detectar los siguientes tipos de tráfico:
  a. Bots buenos / Bots malos
  b. Bots de confianza y semi-confianza
  c. Agregadores
  d. Raspadores de contenido (content scrapers)
  e. Rastreadores de búsqueda
  f. Herramientas de contraseña
  g. Aplicación DDoS
  h. Prueba interna / desarrollo
- La solución SaaS debe ofrecer las siguientes opciones para el cumplimiento de las políticas:

a. Bloqueo
b. Redirigir
c. Reenviar
d. Responder directamente desde el dispositivo
e. Engañar
f. Permitir en solo lectura
g. Limitación de tarifas (rate limit) basada en decisiones comerciales
h. Marcar el tráfico para acciones de seguimiento y listas de vigilancia
i. Trabajar con aplicaciones para diseñar interacciones particulares o invocar una lógica de aplicación alternativa

- La solución SaaS NO puede depender de CAPTCHAS para bloqueo o identificación de automatización
- La solución SaaS debe ofrecer dos modos de implementación: basada en la nube (alojada) y local (on premise)
- La solución SaaS debe estar disponible como un servicio administrado
- La solución SaaS debe demostrar que incluye protección contra ingeniería reversa y ofuscación del JavaScript y SDK.
- La solución SaaS debe generar dinámicamente un JavaScript único para cada cliente.
- La solución SaaS debe incluir JavaScript y/o SDK para la recopilación avanzada de señales y la detección de bots y estafadores sofisticados.
- La solución SaaS debe formar parte de una plataforma de servicios que también incluya soluciones para la mitigación del fraude manual, así como soluciones para mejorar la experiencia del cliente por reducción de fricción (en la misma plataforma de servicios gestionados, por el mismo proveedor)
- La solución SaaS debe de ser administrada de forma centralizada, con reglas comerciales flexibles para adaptarse a los canales comerciales.
- La solución SaaS debe soportar diferentes tecnologías web y Móviles (iOS y Android).
- La solución SaaS debe proporcionar implementación perimetral y cambios mínimos en la aplicación.
- La solución SaaS debe proporcionar categorización de tipos de automatización. No debe ser una solución SaaS basada en firmas (signature based).
- La solución SaaS no debe depender de la colección de PII para detección de automatización.
- La solución SaaS debe proporcionar anonimización en los métodos de recopilación de datos.
- La solución SaaS debe proporcionar la capacidad de rastrear el historial del usuario y/o del dispositivo.
- La solución SaaS debe poder rastrear los usuarios, dispositivos y las cuentas a las que acceden.
- La solución SaaS no debe interferir con el rendimiento de la aplicación si hay problemas de conectividad a Internet.

- La solución SaaS debe soportar aplicaciones móviles híbridas (nativas y Webview).
- En caso de que el proveedor ofrezca un servicio SaaS integral, gestionando completamente los servicios de seguridad, el monitoreo de la disponibilidad y resolución de problemas se presentará en un Acuerdo de Nivel de Servicio (SLA) con reportes mensuales, y adicionales a solicitud, sobre el estado del servicio. Al asumir el proveedor la responsabilidad total de la administración de la seguridad y contar con un equipo de respuesta ante incidentes 24x7, los puntos mencionados en el apartado 11.3 no serán considerados. Esta modalidad solo será aceptada en la implementación SaaS integral en la nube.

11.6. Plataforma de Protección Nativa de Nube para Aplicaciones (CNAPP)

El Banco requiere que, como parte de la implementación de la Plataforma Bancaria, esta sea protegida por una plataforma de protección nativa de nube para aplicaciones (CNAPP) que tenga las siguientes características:

- Seguridad para las cargas de trabajo que se van migrando y desarrollando en ambientes cloud (AWS, Azure, GCP, OCI).
- Incluir controles en todo el ciclo de vida de la aplicación: Codificación y Desarrollo, Despliegue, ejecución, entre otros.
- Una plataforma consolidada que pueda ofrecer todas las capacidades en una sola consola.
- Cumplimiento de las siguientes protecciones por cada una de las siguientes etapas:

a) Etapa de Codificación y Desarrollo

- Debe escanear plantillas de Infraestructura como Código (IaC), incluyendo: Terraform, Cloudformation, Azure Resource Manager (ARM), Helm, DockerFiles, Manifiestos de Kubernetes (yaml), archivos Swagger, BICEP.
- Debe escanear cada módulo de IaC (cómo los módulos de Terraform)
- Debe escanear los bloques dinámicos de Terraform.
- Debe hacer remediación y, de ser posible inclusive, accionar remediación automática.
- Debe detectar y escanear plantillas de IaC existentes en repositorios Git (como, por ejemplo: GitHub, Gitlab, BitBucket, Azure Repos).
- Debe mostrar la relación entre los elementos del código, como, por ejemplo, las plantillas de IaC y los paquetes utilizados, para determinar su relación y sus dependencias.
- Debe detectar errores en las configuraciones de IaC en los "Pull Request" y "Merge Request".
- Debe crear y modificar reglas personalizadas para escaneo de IaC.

- Debe hacer "Drift Detection" entre las plantillas de IaC y lo que realmente está desplegado en el proveedor de nube.
- Debe escanear los repositorios Git existentes en búsqueda de vulnerabilidades y compliance en código.
- Debe detectar vulnerabilidades en paquetes, tales como Docker, Go, Java (Maven/Gradle) Javascript (NPM, Yarn, Bower) Kotlin (Gradle) Python (Pip, Pipfile), Ruby, y YAML.
- Debe escanear vulnerabilidades basadas en CVEs y que brinde información de cada vulnerabilidad (ejemplo: CVE ID, puntaje CVSS, nombre del paquete, versión, vectores de ataque, y si existe o no un "fix").
- Debe proporcionar escaneo para incumplimiento de compliance de licencias.
- Debe escanear paquetes luego de un "Pull Request” y "Merge Request".
- Debe generar listas de materiales de software (SBOM) en formatos estándar de la industria (por ejemplo, Cyclone DX XML y CSV)
- Debe tener la capacidad de remediar vulnerabilidades mediante el bump de versiones de paquetes.
- Debe identificar patrones de vulnerabilidades comunes identificados en la industria, como los OWASP top 10 y CWE top 25.
- Debe identificar vulnerabilidades y patrones que causan vulnerabilidades en el código fuente y permitir solucionar problemas de forma proactiva antes de que lleguen a producción.
- Debe incluir licenciamiento para soportar lenguajes modernos como Java, JavaScript, Python, TypeScript y Go.
- Debe permitir a los desarrolladores solucionar problemas durante el desarrollo, incorporando comentarios de seguridad en IDEs, proveedores de VCS y pipelines de CI/CD, como para monitorear continuamente el código a medida que se escribe y proporcionar correcciones de seguridad en línea.
- Debe proporcionar guardrails para bloquear los PRs si estos introducen debilidades críticas.
- Debe integrarse con los flujos de trabajo de desarrolladores y con herramientas nativas.
- Debe integrarse con línea de comandos e IDE (ej., VSCode e IntelliJ)
- Debe Integrarse con herramientas SCR (repositorio de código fuente), incluidos GitHub y GitLab.
- Debe integrarse directamente con herramientas de CI/CD Pipelines (por ejemplo, Github Actions, Azure DevOps, Jenkins).
- Debe integrarse con herramientas de línea de comandos y workflows preestablecidos.
- Debe integrarse dentro de los Git pre-commits
- Debe realizar escaneo de secretos, detección de secretos en IDEs, repositorios Git y herramientas de CI/CD.

- Debe mostrar gráficos de plantillas y paquetes de Código, resaltando las dependencias o los recursos implementados a partir de las plantillas.
- Debe reportar los resultados de los escaneos dentro de las herramientas de los desarrolladores [por ejemplo, Git (Github, Gitlab), herramientas IDE y herramientas de CI]
- Debe permitir crear políticas personalizadas, además de políticas predefinidas.
- Debe proporcionar una visualización de "Software Supply Chain", con detalle de las dependencias.
- Debe permitir etiquetado de los recursos de infraestructura como código.

b) Etapa de Despliegue

- Debe Integrarse con registros de contenedores para escanear vulnerabilidades y compliance una vez las imágenes son construidas.
- Debe incluir escaneo de cumplimiento de licenciamiento Open Source.
- Debe incluir escaneo de vulnerabilidades en los pipelines para aplicaciones contenerizadas, paquetes de software (ejemplo Python, Java, Go) y funciones serverless (ejemplo, AWS Lambda, Azure Functions, GCP Functions).
- Debe incluir escaneo de imágenes de contenedores en un Sandbox al descargarlas de terceros para identificar comportamientos maliciosos (ej., malware, criptomineros, comando y control saliente), así como el comportamiento de las imágenes de contenedores (ej., procesos, llamadas al sistema de archivos).
- Debe Integrarse con herramientas y registros de CI conocidos (ej., GitHub Actions, Azure DevOps, Jenkins).
- Debe generar reportes de los resultados directamente en los pipelines sin que los desarrolladores tengan que acceder a herramientas de seguridad separadas.
- Debe poder intervenir (bloquear) los pipelines si se infringen los umbrales configurados (por ejemplo, vulnerabilidades críticas, como Log4J, cumplimiento de licencias, incumplimiento de los estándares de la empresa).
- Debe realizar escaneo de secretos en pipelines, y detectar secretos durante la ejecución del pipeline y parar el pipeline en caso se detecten secretos.

c) Etapa de Ejecución

- Debe permitir la integración con los siguientes cloud service providers: GCP, AWS, AZURE, Alibaba Cloud, OCI, IBM Cloud.
- Debe ofrecer visualización de recursos a través de múltiples proveedores de nube en una sola consola.
- Debe incluir el poder reflejar rápidamente los principales riesgos de los activos y priorizar las amenazas en dashboards ejecutivos.

- Debe incluir el poder admitir varias cuentas del mismo proveedor o de varios proveedores (por ejemplo, suscripciones y tenants de Azure, cuentas y organizaciones de AWS, organizaciones y proyectos de GCP).
- Debe incluir el poder filtrar por tipos de recursos: por ejemplo, tipos de instancias (EC2, imágenes de VM), IAM, almacenamiento (buckets, Blob Storages, Block Storages), bases de datos, VPC, Serverless, clústeres de Kubernetes].
- Debe incluir el poder proporcionar datos de configuración detallados para cada recurso.
- Debe incluir el poder almacenar la última configuración para cada recurso
- Debe incluir el poder proporcionar un historial de cambios detallado para los recursos desplegados, además de la capacidad de identificar el cambio junto con la nueva configuración para el recurso.
- Debe incluir el poder filtrar los recursos por variables que incluyen cambio de hora, región, cuenta (suscripción, organización, proyecto), tag o etiqueta.
- Debe supervisar las actividades de administrador, operador y roles automatizados en todas las plataformas en la nube.
- Debe permitir investigar el acceso desde regiones desconocidas y que genere alertas cuando detecta comportamientos inusuales (por ejemplo, iniciar sesión como root).
- Debe detectar modificación de permisos a un recurso.
- Debe incluir el poder hacer análisis de comportamiento del usuario (UEBA) para detectar actividades inusuales (por ejemplo, actividades sospechosas, inicios de sesión fallidos, patrones de actividad inusuales para un usuario)
- Debe incluir el poder crear o modificar validaciones y políticas específicas de la organización.
- Debe incluir el poder Supervisar y detectar cambios en las funciones Serverless (ej., eliminar, ejecutar y modificar funciones).
- Debe incluir el poder Supervisar todos los tipos de nubes en busca de actividad inusual en función de los datos de flujo de la red (flow logs).
- Debe incluir el poder Alertar sobre el tráfico de red que fluye desde direcciones de origen sospechosas.
- Debe incluir el poder Visualizar el tráfico que fluye a través de grupos de seguridad mal configurados.
- Debe incluir el poder Identificar el flujo de tráfico a los recursos en los puertos expuestos (por ejemplo, MySQL, SSH, Telnet, RDP).
- Debe incluir el poder Detectar instancias expuestas conectadas directamente a Internet.
- Debe incluir el poder Detectar minería de criptomonedas.
- Debe incluir el poder Analizar los flujos para cualquier tráfico C2.
- Debe incluir el poder Modificar o crear verificaciones y políticas de red específicas de la organización.
- Debe incluir el poder filtrar alertas por VPC, región de la nube, origen (bytes enviados y recibidos) en función de grupos de seguridad y etiquetas

- Debe incluir el poder proporcionar líneas de base listas para usar contra estándares y marcos bien conocidos, debe incluir CIS, NIST (CSF y 800-53 Series), ISO 27001, GDPR, PCI DSS 3.2, SOC 2, HITRUST, Mitre ATT&CK, CCPA.
- Debe incluir el poder crear estándares de cumplimiento personalizados, específicos de la organización.
- Debe incluir el poder Profundizar en los detalles y comprender rápidamente el incumplimiento de los estándares.
- Debe incluir el poder Modificar las políticas y verificaciones existentes para cumplir con los requisitos específicos de la organización.
- Debe incluir el poder Escanear de forma continua y automática para verificar el cumplimiento sin requerir que los operadores configuren y programen escaneos manuales.
- Debe incluir el poder Generar informes de nivel ejecutivo que se pueden personalizar para cuentas en la nube, proyectos, subs, rango de datos, regiones, cuentas, grupos de cuentas (por ejemplo, desarrollo, producción) específicos dentro del alcance.
- Debe incluir el poder Crear reglas adicionales para determinar instancias (mejores prácticas), si las etiquetas están asociadas con recursos, mejores prácticas de usuario (ej., rotación de contraseñas, MFA), almacenamiento (ej., cifrado en reposo), configuración de red (ej., grupos de seguridad, VPC), clústeres de Kubernetes, configuración en recursos Serverless.
- Debe incluir el poder actualizar políticas de estándares existentes con reglas y políticas personalizadas.
- Debe incluir el poder aplicar o modificar la severidad de las políticas y verificaciones personalizadas y existentes.
- Debe incluir el poder garantizar el cumplimiento continuo sin tener que configurar o modificar constantemente los escaneos una vez que se incorporan las cuentas en la nube.
- Debe incluir el poder remediar automáticamente el incumplimiento de la configuración de algún recurso.
- Debe incluir el poder filtrar por la gravedad del incumplimiento.
- Debe incluir el poder exportar eventos de incumplimiento a través de API, CSV o integración con otras plataformas [por ejemplo, Slack, SOAR, Jira y correo electrónico].
- Debe incluir el poder Filtrar e identificar verificaciones de cumplimiento específicas por nombre, recurso afectado, severidad u otras métricas (por ejemplo, cuentas en la nube, etiquetas).
- Debe incluir el poder Proporcionar actualización automática de las políticas de configuración y cumplimiento.
- Debe incluir el poder Analizar los privilegios de IAM en varios proveedores de nube (p. ej., GCP, AWS y Azure).
- Debe incluir el poder Evaluar las identidades y roles de IAM para garantizar que se sigan las mejores prácticas y los principios de privilegios mínimos,

incluida la capacidad de descubrir identidades con políticas demasiado permisivas, acceso "wildcard" a los recursos, acceso público permitido y cuándo se utilizó por última vez el acceso y la identidad con los permisos asignados.

- Debe incluir el poder crear reglas personalizadas de IAM para buscar permisos específicos y si se están usando o no.
- Debe incluir el poder Proporcionar reglas listas para usar que tengan en cuenta la complejidad de IAM (por ejemplo, cuentas con acceso "wildcard", acceso entre cuentas, privilegios excesivos durante un período, acceso no utilizado o demasiado permisivo).
- Debe incluir el poder crear políticas personalizadas o la capacidad de modificar políticas existentes.
- Debe incluir el poder visualizar en un gráfico, tabla la relación entre roles y recursos con acceso.
- Debe incluir el poder filtrar o visualizar rápidamente alertas y eventos basados en IAM.
- Debe incluir el poder corregir de problemas basados en IAM durante la compilación o el tiempo de ejecución.
- Debe incluir el poder Proporcionar políticas de tiempo de compilación para solucionar problemas relacionados con IAM al principio del proceso de compilación.
- Debe incluir el poder integrarse con herramientas de SSO, como Okta y Azure AD.
- Debe incluir el poder realizar investigaciones personalizadas para buscar problemas específicos de IAM dentro de una organización.
- Debe incluir el poder validar objetos en servicios de almacenamiento (por ejemplo, Buckets S3 de AWS y Azure Blob Storage) e informar sobre configuraciones incorrectas (por ejemplo, exposición pública), malware dentro del objeto y políticas o problemas de datos que surgen de los datos almacenados dentro del depósito (por ejemplo, violaciones de cumplimiento con GDPR, PCI).
- Debe incluir el poder escanear el almacenamiento de objetos para decidir qué buckets se escanean y cuántos datos se escanean.
- Debe incluir el poder escanear datos existentes y nuevos enviados a servicios de almacenamiento.
- Debe incluir el poder Identificar infracciones de cumplimiento en hosts en ejecución existentes dentro del entorno.
- Debe incluir el poder escanear todas las imágenes del host (sistemas operativos) en busca de infracciones de cumplimiento, independientemente de si se implementan en entornos de nube pública, on-premises o híbridos.
- Debe incluir el poder Proporcionar líneas base listas para usar contra estándares bien conocidos (por ejemplo, CIS, Docker y Kubernetes, NIST 800-190, PCI, GDPR) y marcos para hosts, incluidos Windows, Linux, Docker host (daemon y operaciones de seguridad) y Kubernetes.

- Debe incluir el poder Realizar comprobaciones para ver la configuración del host de Windows del Firewall de Windows, Windows Defender (antimalware) y la configuración de actualización de Windows.
- Debe incluir el poder monitorear la integridad de archivos (FIM) de archivos y directorios.
- Debe incluir el poder Identificar automáticamente las infracciones de cumplimiento de las funciones "Serverless", incluidas las claves y contraseñas privadas incrustadas, el acceso demasiado permisivo, el acceso amplio a los recursos, los servicios no utilizados a los que puede acceder la función y las acciones de funciones sospechosas.
- Debe incluir el poder escanear todas las imágenes de contenedores en busca de infracciones de cumplimiento, independientemente de si se implementan en entornos de nube pública, on-premises, híbridos o ambientes aislados (air-gapped).
- Debe incluir el poder proporcionar un escaneo de cumplimiento que no requiera cambios en la imagen del contenedor a través de la inserción de agentes o mecanismos similares (agentless).
- Debe incluir el poder Proporcionar referencias listas para usar con marcos y estándares bien conocidos para imágenes de contenedores, tiempo de ejecución y configuración de Kubernetes, como CIS (Docker y Kubernetes), NIST 800-190, PCI y GDPR.
- Debe incluir el poder Realizar una auditoría de cumplimiento en la fase de CI de compilación de DevOps (pipelines) (por ejemplo, Jenkins, CircleCI, Azure DevOps) y proporcionando métricas de vulnerabilidad dentro de la plataforma de compilación con la opción de fallar la compilación si se viola el cumplimiento de un se descubre la severidad dada.
- Debe incluir el poder Escanear una imagen de contenedor "standalone" antes de registrarse en un registro, construir una canalización o ejecutar.
- Debe incluir el poder Escanear registros de contenedores (registries) para garantizar el cumplimiento continuo de las imágenes (por ejemplo, Azure Container Registry, Docker Hub, Google Container Registry, registro de contenedores AWS EC2, Nexus Sonar y JFrog)
- Debe incluir el poder Identificar infracciones de cumplimiento en contenedores en ejecución existentes dentro del entorno
- Debe incluir el poder Proporcionar la capacidad de visualizar de manera concisa las infracciones de cumplimiento en la construcción, implementación y ejecución
- Debe incluir el poder Configurar políticas proactivas para alertar o evitar la implementación de imágenes no compatibles en un entorno de producción
- Debe incluir el poder restringir el uso solo a "imágenes confiables"
- Debe incluir el poder Supervisar la integridad de los archivos de los contenedores en ejecución para garantizar la detección y la prevención de escrituras o accesos no autorizados al sistema de archivos.

- Debe incluir el poder Comprender cada falla de cumplimiento (por ejemplo, facilidad de ataque, vectores de amenazas, si hay una solución disponible y cuánto tiempo ha existido la violación).
- Debe incluir el poder Escanear todos los hosts compatibles en busca de vulnerabilidades, independientemente de si se implementan en entornos de nube pública, on-premises o híbridos
- Debe incluir el poder Identificar vulnerabilidades corriendo en los hosts (sistemas operativos)
- Debe incluir el poder identificar automáticamente las vulnerabilidades de las funciones Serverless, incluidas las vulnerabilidades en las librerías de las funciones.
- Debe incluir el poder Escanear las vulnerabilidades de la imagen del contenedor sin necesidad de realizar cambios en la imagen mediante la inserción de agentes o un mecanismo similar
- Debe incluir el poder Escanear todas las imágenes de contenedores en busca de vulnerabilidades, independientemente de si se implementan en entornos de nube pública, on-premises o híbridos
- Debe incluir el poder Escanear una imagen de contenedor "standalone" antes de registrarse en un registro, en CI (pipeline) o ya corriendo.
- Debe incluir el poder Escanear registros de contenedores (por ejemplo, Azure Container Registry, Docker Hub, Google Container Registry, registro de contenedores AWS EC2, Nexus Sonar y JFrog) para garantizar el estado continuo de las imágenes de contenedores
- Debe incluir el poder Descubrir vulnerabilidades de imágenes de contenedores dentro del entorno ya corriendo.
- Debe incluir el poder Profundizar en la imagen de cada contenedor para visualizar las capas exactas donde existen vulnerabilidades y permitir comentarios rápidos a través de la integración con los flujos de trabajo de DevOps
- Debe incluir el poder comprender cada vulnerabilidad en profundidad, así como los vectores de amenazas que podrían aumentar el perfil de riesgo en el entorno (ej., facilidad de ataque, si hay una solución disponible, cuánto tiempo ha existido la vulnerabilidad, características de ejecutar contenedores que elevan el riesgo, CVE detallado información y detalles de remediación, los contenedores y hosts en los que existe la vulnerabilidad, los paquetes y marcos afectados, y el porcentaje de entorno afectado)
- Debe incluir el poder Configurar políticas proactivas para alertar o evitar la implementación de imágenes de contenedores vulnerables en un entorno de producción
- Debe incluir el poder Ajustar las políticas en función del nivel de gravedad, las etiquetas, las imágenes y otros factores.
- Debe incluir el poder Proporcionar un mecanismo para actualizar las firmas de vulnerabilidad en entornos aislados (air-gapped)

- Debe incluir el poder Proporcionar métricas de vulnerabilidad directamente dentro de la plataforma de compilación, junto con la opción de fallar la compilación (CI) si se descubren vulnerabilidades de una gravedad determinada.
- Debe incluir el poder Proporcionar una visualización de alto nivel de cualquier vulnerabilidad que exista
- Debe incluir el poder Filtrar según la gravedad de la vulnerabilidad
- Debe incluir el poder Realizar una evaluación de vulnerabilidades en la fase de CI de la canalización de compilación de DevOps conectándose a plataformas de compilación conocidas (por ejemplo, Jenkins, CircleCI y Azure DevOps)
- Debe incluir el poder Exportar información de evaluación de vulnerabilidades a través de API, CSV o integración con otras plataformas [por ejemplo, Slack, SOAR, Jira, correo electrónico]
- Debe incluir el poder Filtrar vulnerabilidades según criterios específicos (es decir, número CVE)
- Debe incluir el poder Actualizar automáticamente las fuentes de vulnerabilidades sin sobrecarga operativa
- Debe incluir el poder realizar Mapeo contra estándares y métricas de vulnerabilidad bien conocidas (por ejemplo, CVE) y use mecanismos de puntuación comunes (por ejemplo, CVSS)
- Debe incluir el poder realizar escaneos de vulnerabilidades ya sea a través de agentes o sin agentes.
- Debe incluir el poder importar datos de vulnerabilidad de los sistemas de clientes existentes (p. ej., Qualys, Tenable, Guard Duty)
- Debe incluir el poder escanear paquetes (p. ej., Python, Java y Go) antes de implementarlos en la nube pública o antes de que se conviertan en imágenes de contenedores
- Debe incluir el poder aplicar reglas de vulnerabilidad cuando haya soluciones de proveedores disponibles. Si un CVE no tiene "fix" no debería bloquear.
- Debe incluir el poder Hacer observaciones del host (ej., cuando se ejecutan aplicaciones, eventos SSH y actualizaciones de seguridad)
- Debe incluir el poder crear reglas de host para monitorear, alertar y prevenir actividades específicas (por ejemplo, malware, criptominería, herramientas de explotación, acceso persistente, ataques de contraseña, rastreo y suplantación de identidad)
- Debe incluir el poder Mapear y aprender automáticamente la actividad de la red entre los hosts en el entorno
- Debe incluir el poder Descubrir automáticamente violaciones de cumplimiento para funciones Serverless que podrían generar incidentes, incluidas claves y contraseñas privadas incrustadas, acceso demasiado permisivo, acceso amplio a recursos, servicios no utilizados a los que puede acceder la función y acciones de funciones sospechosas.

- Debe incluir el poder Proteger las funciones Serverless (por ejemplo: red, procesos) para ayudar a prevenir el abuso
- Debe incluir el poder Establecer líneas de base (baseline) para imágenes de contenedores y sus comportamientos esperados (a través de la actividad de la red, procesos, llamadas al sistema, sistema de archivos) a través de una combiNación de análisis estático de los Dockerfile y el manifiesto de despliegue, y el análisis dinámico de un contenedor en ejecución.
- Debe incluir el poder Establecer un proceso para re-aprendizaje de la línea base de las imágenes de contenedores, e informar cuando la actividad sea anormal o se desvíe de la línea de base (por ejemplo, nuevo proceso generado, comunicaciones de red que difieren de la línea de base, acceso ejecutivo a contenedores)
- Debe incluir el poder enviar Imágenes de contenedor a un sandbox cuando se descargan de registros de terceros para detectar comportamiento malicioso o malware antes de su uso
- Debe incluir el poder Proporcionar protección proactiva contra ciertos incidentes, incluida la capacidad de prevenir procesos no autorizados y actividad de red o, en casos extremos, a través de una política flexible que se puede personalizar en función de las imágenes, namespaces o las etiquetas del contenedor, para finalizar un contenedor en ejecución.
- Debe incluir el poder Mapear y aprender automáticamente la actividad de la red entre las imágenes del contenedor en el entorno
- Debe incluir el poder Proporcionar protección de aplicaciones web de capa 7 para contenedores (por ejemplo, protección CSRF, protección XSS, protección contra inyección SQL, protección contra herramientas de ataque, protección contra solicitudes con formato incorrecto)
- Debe incluir el poder definir reglas para monitorear y alertar sobre el tráfico de la red, incluidas las IP sospechosas basadas en fuentes de amenazas, direcciones IP, rangos o puertos específicos y tráfico DNS sospechoso.
- Debe incluir el poder Supervisar registros específicos y actividad de archivos, según lo definido por una política personalizada
- Debe incluir el poder Proporcionar protección proactiva contra ciertos incidentes, incluida la capacidad de alertar sobre aplicaciones no autorizadas en los hosts.
- Debe incluir el poder incluir inteligencia de amenazas para detectar comportamientos maliciosos o anormales (por ejemplo, cripto-minería, malware, comunicación con dominios y destinos de alto riesgo, movimiento lateral)
- Debe incluir el poder Profundizar en incidentes para realizar investigaciones forenses y capturar y exportar información relacionada con el incidente
- Debe incluir capacidades de firewall nativas de la nube para denegar o permitir explícitamente la conectividad de red.
- Debe incluir el poder describir activamente cargas de web y basadas en API implementadas que no están siendo protegidas.

- Debe incluir el poder Proporcionar protección para aplicaciones web a nivel de capa 7 para contenedores, máquinas virtuales, funciones Serverless y nodos subyacentes.
- Debe incluir el poder elegir si se quiere activar la característica de protección de aplicaciones Web y API in-line (para proteger) o out-of-band (para monitorear únicamente)
- Debe incluir el poder Activar la visibilidad y la protección para rutas web específicas y API Endpoints
- Debe incluir el poder hacer inspección de TLS de aplicaciones Web y API endpoints.
- Debe incluir soporte para HTTP y HTTP 2 y poder definir puertos de escucha.
- Debe incluir el poder importar definiciones API a través de formatos OpenAPI/Swagger.
- Debe incluir el poder prevenir ataques del OWASP y API Top 10 - riesgos de inyección de SQL
- Debe incluir el poder proteger de ataques de DoS (Denegación de Servicio) con excepciones.
- Debe incluir el poder Bloquear el tráfico de ubicaciones de origen no deseadas y prohibidas según el rango de IP y los países de origen
- Debe incluir el poder de hacer detección activa y pasiva, y prevención contra bots
- Debe incluir el poder de detectar bots nuevos o desconocidos utilizando una serie de mecanismos de desafío, incluida la detección de cookies, la inyección de JavaScript y ReCAPTCHA.
- Debe incluir la capacidad de definir bots amigables utilizados activamente dentro de la organización.
- Debe permitir generar alertas activas y detalles de eventos para cada alerta generada
- Debe permitir se apliquen reglas personalizadas o definidas por el usuario tanto a las solicitudes como a las respuestas
- Debe permitir activamente proteger API endpoints.
- Debe incluir el poder para integrar múltiples nubes públicas (AWS, Azure, GCP, OCI, Alicloud, IBM Cloud)
- Debe incluir el poder integrar cuentas de nube pública tanto vía Web (GUI) como vía API.
- Debe incluir el poder agrupar cuentas de nube con el fin de poder filtrar y asociarlas con RBAC.
- Debe incluir el poder tener una guía para el usuario con los siguientes pasos recomendados para mejorar la seguridad y la postura de su ambiente.
- Debe incluir el poder crear un modelo RBAC detallado para la separación de funciones y datos (p. ej., sólo lectura, rol para agregar cuentas en la nube, acceso limitado a cuentas o grupos de cuentas específicos y flexibilidad para crear roles personalizados y conjuntos de permisos)

- Debe incluir el poder integrarse con SSO y proveedores de Federación a través de protocolos estándares de la industria (ejemplo, SAML)
- Debe incluir el poder enviar alertas a herramientas de flujo de trabajo de terceros además de visualizaciones en el producto [por ejemplo, Slack, plataformas SIEM (Splunk | Qradar), Jira, correo electrónico, ServiceNow y herramientas nativas de la nube (Amazon SQS | CSCC), SOAR y Webhooks]
- Debe incluir el poder ajustar las alertas generadas y personalizar el tipo de alertas enviadas a las herramientas y equipos de flujo de trabajo relevantes
- Debe estar licenciado para Soportar API RESTful estándar de la industria
- Debe incluir el poder remediar directamente hallazgos de seguridad o a través de la integración con otras herramientas de flujo de trabajo.
- En caso de que el proveedor ofrezca un servicio SaaS integral, gestionando completamente los servicios de seguridad (incluyendo CNAPP), deberá entregar informes mensuales sobre incidencias y seguridad, así como informes adicionales a solicitud. Al asumir el proveedor la responsabilidad total de la administración de la seguridad y contar con un equipo de respuesta ante incidentes 24x7, los puntos mencionados en el apartado 11.6 podrían no considerarse. Esta modalidad solo será aceptada en la implementación SaaS integral en la nube.

11.7. Servicio de Next Generation Firewall (NGFW)

alertas enviadas a las herramientas y equipos de flujo de trabajo relevantes
El BANCO solicita la adquisicion de una solución de Next Generation Firewall (NGFW) para la seguridad de la información de los servicios del proveedor de nube del Banco de la Nación. La solución debe incluir filtro de paquetes, control de aplicaciones, IPS, prevención contra amenazas de virus, spyware, malware, explotación de vulnerabilidades y command and control para los distintos flujos de tráfico de los servicios en el proveedor de nube del Banco: tráfico inbound y outbound hacia y desde internet y el data center, así como también el tráfico este-oeste de una nube privada virtual a otra.

a) Datos Generales

- La solución debe consistir de una solución de Cloud Next Generation Firewall (NGFW) nativo, en el proveedor de servicios de nube, integrado en cada zona de disponibilidad requerida por el Banco, implementadas dentro de una nube privada virtual de seguridad, protegiendo los distintos flujos de tráfico desde y hacia nubes privadas virtuales.
- El NGFW debe ser entregado como un servicio de nube, construido en base a escalabilidad completamente automática y resiliente, de tareas administrativas como parchado y actualización de sistema operativo, controlados y operados por el vendor del NGFW de nube. El NGFW de nube debe nativamente integrar sus capacidades, de manera que pueda ser administrado desde la misma consola del proveedor de nube.
- La plataforma debe ser optimizada para análisis de contenido de aplicaciones en Capa 7.

- La solución de seguridad debe estar presente en los últimos 5 reportes de Gartner, en el cuadrante de Lideres para Network Enterprise Firewalls.
- La solución de NGFW debe tener acceso programático para crear y administrar el NGFW y pilas de reglas mediante API REST.
- Mediante el API REST, debe poder invocar acciones en recursos del NGFW de la nube (NGFW y pilas de reglas) a través de una aplicación o herramienta de terceros.
- Mediante el API REST también debería poder utilizar herramientas de infraestructura como código (IAC), como plantillas de CloudFormation (CFT) y plantillas de Terraform. Debe poder instalar y ejecutar estas herramientas de IaC en cargas de trabajo dentro o fuera del entorno de AWS.
- Debe poder utilizarse la función de IAM del proveedor de nube en la cuenta del Banco de la Nación para acceder a las API de Cloud NGFW y debe poder configurar qué recursos de IAM pueden asumir esta función, con el objetivo de mejorar la postura de seguridad general mediante el uso de credenciales temporales y su rotación automática.
- El acceso programático a Cloud NGFW deberá estar deshabilitado de forma predeterminada.

b) Detalle General de la Solución

- La solución debe poder asegurar una cantidad de 12 TB por mes.
- Se deben poder crear un grupo de reglas locales que se administren en una cuenta del Banco en el proveedor de nube.
- Se deben poder crear un grupo de reglas globales que se administren en una organización de la cuenta del Banco en el proveedor de nube.
- Los grupos de reglas locales deben poder ser creadas y administradas por administradores de cuentas locales.
- Los grupos de reglas globales deben ser creadas y administradas por administradores del grupo de reglas globales.
- Se deben poder configurar reglas por jerarquías.
- Las reglas de un grupo de reglas global deben poder actuar como reglas predeterminadas globales para todos los firewalls asociados.
- Las reglas del firewall deben tomar en cuenta dirección IP origen (que puede ser un grupo de direcciones IP), dirección IP destino (que puede ser un grupo de direcciones IP) y servicio (o grupo de servicios) de la comunicación que se está analizando.
- Los firewalls deben detectar y filtrar protocolos de red y conectividad.

c) Control de Aplicaciones

- La solución de NGFW deberá poseer la capacidad de reconocer aplicaciones, independiente del puerto y protocolo.
- Debe inspeccionar el payload del paquete de datos.
- Debe actualizar la base de firmas de aplicaciones automáticamente.

d) Prevención de Amenazas

- La solución debe poseer firmas de prevención de intrusos IPS y Command and Control integrados en la solución.
- Debe incluir firmas de bloqueo de archivos maliciosos.
- Debe permitir el bloqueo de vulnerabilidades.
- Debe permitir el bloqueo de exploits.
- Bloquear ataques efectuados por gusanos.
- La solución debe poder crear perfiles de seguridad en función de la inspección del contenido del tráfico.
- Debe poder escanear el tráfico permitido y bloquear amenazas como virus, malware, spyware y ataques DDOS.
- Debe permitir bloquear los intentos de explotación de las vulnerabilidades y fallas del sistema u obtener acceso no autorizado a los sistemas.
- Debe permitir identificar y bloquear los hosts infectados cuando el tráfico sale de la red.
- Debe poseer firmas para bloqueo de ataques de buffer overflow.
- Debe permitir bloquear la ejecución de código malicioso.
- Debe permitir bloquear el software espía de los hosts comprometidos para que no intente conectarse a servidores externos de comando y control (C2).
- Debe permitir bloquear ataques de fuerza bruta, indicando la frecuencia y el ritmo al que ocurrió la actividad sospechosa.
- Debe permitir bloquear exploit kits para evitar que varias explotaciones de diferentes vulnerabilidades y CVEs puedan ser utilizadas contra los sistemas del Banco.
- Debe permitir bloquear vulnerabilidades de software que un atacante podría aprovechar para robar información confidencial o de propiedad exclusiva.
- Debe detectar y bloquear el uso de contraseñas débiles, comprometidas y predeterminadas del fabricante de software y dispositivos de red.
- Debe detectar y bloquear cuando un host intente conectarse a una página de phishing.
- Debe detectar y bloquear anomalías de protocolo, donde el comportamiento de un protocolo se desvía del uso estándar y compatible.
- Debe bloquear ataques de tipo sql-injection
- Debe detectar y bloquear programas que permitan a un atacante obtener acceso remoto no autorizado a un sistema.
- Debe detectar y bloquear actividad botnet.
- Debe detectar y bloquear cryptominer.
- Debe poseer firmas para bloquear fraude, detectando el acceso a sitios web comprometidos a los que se ha determinado que se les ha inyectado código JavaScript malicioso para recopilar información confidencial del usuario.
- Debe detectar y bloquear el tráfico generado por herramientas de software que utilizan actores maliciosos para realizar reconocimientos, ataques u obtener acceso a sistemas vulnerables.

- Debe bloquear virus, gusanos y troyanos, así como descargas de software espía.
- Debe poder bloquear tipos de archivos específicos en aplicaciones específicas y en la dirección de flujo de sesión especificada (entrante/saliente/ambas).
- Debe permitir bloquear ataques de DoS
- Debe poder permitir el descifrado del tráfico para su inspección.
- Permitir el bloqueo de virus y spywares.
- Debe incluir seguridad contra virus en contenido HTML y JavaScript, software espía (spyware) y worms.
- Seguridad contra descargas involuntarias usando HTTP de archivos ejecutables maliciosos.
- Deberá ser posible definir grupos de aplicaciones en base a sus atributos, por ejemplo, un grupo de aplicaciones de riesgo alto que sea dinámicamente alimentado

e) Administración y Monitoreo

- El NGFW debe poder administrarse desde una consola externa o en la misma consola del proveedor de nube.
- Debe contar con un dashboard interactivo y gráfico que permita monitorear el uso de las aplicaciones en capa 7, actividad por IP (origen y destino), países origen y destino del tráfico, uso de las reglas de seguridad y actividad del tráfico malicioso. Esta información podrá ser vista en base a Bytes y Sesiones, y ser filtrado en base a un rango de tiempo, IP, usuario, país y regla de seguridad.
- Debe permitir el control de acceso a la gestión del equipo a través de roles personalizables.
- Debe soportar la personalización de reportes, permitiendo mostrar información de eventos de antivirus, antispyware, IPS, aplicaciones, malware, debe permitir seleccionar las columnas a mostrar, filtrar la información en base a usuarios, grupos de usuarios, direcciones IP, el rango de fechas de los datos, deben poder ser exportados en PDF y enviados automáticamente vía correo electrónico.
- Con el objetivo de que la institución cuente con autonomía para evaluar si el NGFW se encuentra configurado acorde a las buenas prácticas y evitar que el postor sea juez y parte del control de calidad de ésta, se deberá incluir una herramienta que permita evaluar automáticamente si el NGFW se encuentra configurado acorde a las buenas prácticas del fabricante en materia de los diferentes módulos de seguridad que se le haya activado.
- En caso de que el proveedor ofrezca un servicio SaaS integral, gestionando completamente los servicios de seguridad (incluyendo Firewall), deberá entregar informes mensuales sobre incidencias y seguridad, así como informes adicionales a solicitud. Al asumir el proveedor la responsabilidad total de la administración de la seguridad y contar con un equipo de

respuesta ante incidentes 24x7, los puntos mencionados en el apartado 11.7[14] podrían no considerarse. Esta modalidad solo será aceptada en la implementación SaaS integral en la nube.

11.8. Especificaciones de Capacidades de los Servicios de Seguridad

Leyenda Nomenclaturas:

M	Millones	MB	Megabytes	GB	Gigabytes
TB	Terabytes	HA	High Availability	MS	Milisegundos
TX	Transacciones	VM	Máquina virtual		

Tabla 13:Cruadro de las Especificaciones de Capacidades de los Servicios de Seguridad

Componentes del Servicio	Características	Unidad de medida	Cantidad Mensual Año 1	Cantidad Mensual Año 2	Cantidad Mensual Año 3
Consola SaaS de Seguridad para los servicios WAF, ataques volumétricos de denegación de servicio y servicio de seguridad de APIs.	WAF y DDOS	1 suscripción	1	1	1
	Balanceador para aplicaciones en nube	1 suscripción	4	4	4
	Descubrimiento de APIS en nube	1 suscripción	5	5	5
	Protección de APIS en nube	Tx	340,000	24,000,000	26,400,000
Plataforma de protección nativa de nube para aplicaciones (CNAPP)	Monitoreo de seguridad de red en tiempo real, UEBA e integración con herramientas de administración de vulnerabilidades del host	VM	14	14	14
Servicio de Next Generation Firewall (NGFW)	Software NGFW para gestión de Firewall	Tx	340,000	24,000,000	26,400,000

11.9. Propiedad y Transferencia de la Cuenta de Acceso a los Servicios del PSN

El CONTRATISTA debe de crear la cuenta maestra y todas las secundarias a nombre del BANCO DE LA NACIÓN. Todo servicio, licencia o tecnología desplegada deberá estar a nombre de la BANCO DE LA NACIÓN a través de

[14] Pliego de Consultas N° 01-2024 - Concurso de Méritos (Consulta N° 33 TCO LATAM).

las cuentas del PSN.

El CONTRATISTA también debe transferir la cuenta maestra de gestión de la infraestructura ya sea a la Entidad o a quien la Entidad designe al finalizar el presente contrato. Este acto de entrega representa el fin de las responsabilidades financieras del CONTRATISTA con el Proveedor de Servicios de Nube. En ese momento, ya sea la Entidad o quien este designe, pasará a ser responsable por cualquier elemento técnico relacionado al servicio de nube, así como a los costos asociados con la misma.

El CONTRATISTA debe contar con las credenciales y cumplir con los requisitos y procedimientos exigidos por el PSN para transferir la cuenta maestra dentro de los tiempos señalados en el Contrato.

En caso de que el proveedor entregue todos los servicios de la PSN como parte de una solución SaaS integral gestionada por él mismo, sin costos adicionales por consumo de PSN asociados al contrato, la transferencia de cuentas de PSN no será necesaria. Sin perjuicio a lo anterior, el proveedor ganador de la buena pro, brindará accesos de monitoreo.

12. SEGURIDAD DE LA INFORMACIÓN

1. Código Seguro

- Desarrollo bajo estándares de OWASP Mobile Security y OWASP Web.
- Encriptación de datos End-to-End.
- Control de dispositivos rooteados y con jailbreak.
- Uso de librerías certificadas.
- Conexiones a servidores mediante protocolo TLS 1.3.
- No se almacenan credenciales de acceso en los códigos fuentes, como acceso a bases de datos y otros.
- El control de acceso del dispositivo móvil a la aplicación debe incluir detección y protección con herramientas certificadas[15] ante:
    - Ataques de superposición
    - Ataques de pharming
    - Explotaciones del sistema operativo ("jailbreak", "rooting")
    - Conexiones a redes inseguras (por ejemplo, wi-fi libre)
    - Ejecuciones de la aplicación con pantalla apagada o boca abajo.
    - Detección de reempaquetado de la aplicación móvil
    - Ofuscación de código JavaScript
    - Protección de inyección de código
    - Protección de depuración (Debugger)
    - Protección de captura de pantalla del dispositivo
    - Protección contra el secuestro de tareas en Android (Task hijacking)
    - Protección contra Keylogger en Android.

2. Complementos

[15] Pliego de Consultas N° 01-2024 - Concurso de Méritos (Consulta N° 35 TCO LATAM).

Para la Banca Móvil y la Banca por Internet (de corresponder) se debe incluir la protección con herramientas certificadas de los siguientes puntos[16]:

- Ofuscación: Se utilizarán las reglas nativas para generar un APK seguros.
- Detección de dispositivos rooteados: Se bloqueará el ingreso a la app cuando se detecte un dispositivo rooteado.
- Datos locales se guardan en base de datos nativas (ROOM) de Android.
- No se usarán librerías de dudosa precedencia o que no sean verificadas.
- Codificación bajo los estándares de programación segura por Android.
- Se utilizarán certificados digitales BKS/CERT para crear el cliente HTTPs y establecer la conexión con los webs services mediante TLS.
- No se almacenarán credenciales de acceso en los códigos fuentes, como acceso a bases de datos y otros.
- Detección/protección de reempaquetado de la aplicación móvil.
- Ofuscación de código JavaScript.
- Protección de inyección de código.
- Protección de depuración (Debugger).
- Protección de captura de pantalla del dispositivo.
- Detección de emuladores.
- Protección contra el secuestro de tareas en Android (Task hijacking).
- Protección contra Keylogger en Android.

3. **Sobre OWASP**

El Estándar de Verificación de Seguridad en Aplicaciones (ASVS; por sus siglas en inglés) es una lista de requisitos o pruebas de seguridad en aplicaciones que puede ser utilizado por arquitectos, desarrolladores, probadores, profesionales de la seguridad, proveedores de herramientas y consumidores para definir, construir, probar y verificar aplicaciones seguras.

Una de las mejores maneras de utilizar el estándar de verificación de seguridad en aplicaciones es usarlo como un plano-guía para crear una lista de comprobación de codificación segura específica para su aplicación, plataforma u organización. Adaptar el ASVS a sus casos de uso aumentará el enfoque en los requisitos de seguridad que son más importantes para sus proyectos y entornos.

4. **Niveles de Seguridad**

Nivel 1 (L1)

Primeros pasos, vista automatizada o completa de la cartera Una aplicación alcanza ASVS Nivel 1 si logra defenderse contra vulnerabilidades de seguridad de aplicaciones que son fáciles de descubrir, e incluido el Top 10 de OWASP y otras listas de comprobación similares. El nivel 1 es el mínimo por el que todas las aplicaciones deben esforzarse. También es útil como primer paso en un esfuerzo multifase o cuando las aplicaciones no almacenan ni manejan datos confidenciales y, por lo tanto, no necesitan los controles más rigurosos de Nivel 2 o 3. Los controles de nivel 1 se pueden comprobar automáticamente mediante

[16] Pliego de Consultas N° 01-2024 - Concurso de Méritos (Consulta N° 35 TCO LATAM).

herramientas o simplemente manualmente sin acceso al código fuente. Consideramos el Nivel 1 el mínimo requerido para todas las aplicaciones. Las amenazas a la aplicación probablemente serán de atacantes que utilizan técnicas simples y de bajo esfuerzo para identificar vulnerabilidades fáciles de encontrar y fáciles de explotar. Esto contrasta con un atacante determinado que gastará energía enfocada para apuntar específicamente a la aplicación. Si los datos procesados por su aplicación tienen un alto valor, rara vez querrá detenerse en una revisión de Nivel 1.

Nivel 2 (L2)

Para la mayoría de las aplicaciones Una aplicación alcanza ASVS Nivel 2 (o Estándar) si se defiende adecuadamente contra la mayoría de los riesgos asociados con el software hoy en día. El nivel 2 garantiza que los controles de seguridad estén en su lugar, sean eficaces y se utilicen dentro de la aplicación. El nivel 2 suele ser adecuado para aplicaciones que manejan importantes transacciones de negocioa-negocio, incluidas aquellas que procesan información de atención médica, y/o implementan funciones críticas para el negocio, o procesan otros activos sensibles, o industrias donde la integridad es una faceta crítica para proteger su negocio, como la industria de juegos para frustrar a los tramposos y game hacks. Las amenazas a las aplicaciones de nivel 2 suelen ser atacantes calificados y motivados que se centran en objetivos específicos utilizando herramientas y técnicas, que son altamente practicadas y eficaces para descubrir y explotar las debilidades dentro de las aplicaciones.

Nivel 3 (L3)

Alto valor, alta garantía o seguridad ASVS Nivel 3 es el nivel más alto de verificación dentro del ASVS. Este nivel se reserva normalmente para aplicaciones que requieren niveles significativos de verificación de seguridad, como los que se pueden encontrar dentro de áreas de militar, salud y seguridad, infraestructura crítica, etc. Las organizaciones pueden requerir ASVS Nivel 3 para aplicaciones que realizan funciones críticas, donde el error podría afectar significativamente las operaciones de la organización, e incluso su supervivencia. A continuación, se proporcionan instrucciones de ejemplo sobre la aplicación del nivel 3 de ASVS. Una aplicación alcanza ASVS Nivel 3 (o Avanzado) si se defiende adecuadamente contra vulnerabilidades avanzadas de seguridad de aplicaciones y también demuestra principios de buen diseño de seguridad. Una aplicación en ASVS Nivel 3 requiere un análisis más detallado de la arquitectura, la codificación y las pruebas que todos los demás niveles. Una aplicación segura se modulariza de una manera significativa (para facilitar la resiliencia, la escalabilidad y, sobre todo, las capas de seguridad), y cada módulo (separado por conexión de red y/o instancia física) se encarga de sus propias responsabilidades de seguridad (defensa en profundidad), que deben documentarse correctamente. Las responsabilidades incluyen controles para garantizar la confidencialidad (por ejemplo, cifrado), integridad (por ejemplo, transacciones, validación de OWASP Application Security Verification Standard 4.0.3 (es) 13 entradas), disponibilidad (por ejemplo, manejo correcto de la carga), autenticación (incluidos entre sistemas), autorización y auditoría (registros de

log).

El Desarrollo para el BN debe corresponder al nivel de seguridad más elevado: Nivel 3 (L3)

Se utilizarán los estándares de seguridad en el ciclo de vida de desarrollo de software requeridos por la SBS: OWASP ASVS (aplicación web) - Versión L3 provistos en el ANEXO I OWASP (Application Security Verification Standard 4.0.3 Final octubre 2021)

13. DESARROLLO DE APIs

El sistema implementado debe facultar a los usuarios para llevar a cabo operaciones mediante la interacción con el orquestador y el API Gateway del Banco de la Nación. El orquestador, en este contexto, sirve como intermediario, facilitando la comunicación entre aplicaciones y sistemas bancarios mediante tecnologías como API, Webservices o SOAP. Estos mecanismos son fundamentales para asegurar una comunicación eficaz y segura entre los diversos componentes del sistema.

Sin perjuicio a lo anterior, la nueva plataforma de los canales digitales del Banco de la Nación debe tener la capacidad de integrarse con diversas plataformas del Banco, tanto internas como externas. En este sentido, el Contratista deberá contemplar y asumir el desarrollo e implementación (cloud, onpremise y mainframe) de las siguientes APIs:

- API Login
- API Generar clave de internet
- API transferencia mismo Banco
- API Retiro sin tarjeta
- API Transferencia Interbancaria Inmediata
- **Y otras APIs que se identifiquen durante el desarrollo del proyecto dentro del alcance (Ver anexo N° 1), previa aprobación expresa del Banco.**

El Contratista está encargado de desarrollar los APIs necesarios para el proyecto. El costo de estos APIs debe estar incluido en los costos totales de desarrollo e implementación de la nueva plataforma de los Canales Digitales del Banco de Nación y no será sujeto a pagos diferenciados.

14. SOPORTE TÉCNICO

14.1. Soporte Técnico del Servicio de Nube

Se proveerá un servicio de mantenimiento y soporte bajo las siguientes características:

- En caso se presentar una falla en el servicio, el BANCO podrá comunicarse con el CONTRATISTA a través del Help Desk del Contratista o a través de un envío por correo electrónico el cual será provisto en el plan de trabajo, todas las incidencias y/o requerimientos.
- El CONTRATISTA brindará el servicio de mantenimiento y soporte presencial cuando el Banco lo requiera y sea para la atención de los

componentes ubicados en las instalaciones de BANCO, para los casos de infraestructura pública o nube pública la atención será de manera remota.

- El CONTRATISTA debe tener la capacidad suficiente para la atención y resolución de todos los problemas que se presenten con la solución propuesta y que el Contratista no esté en la capacidad de resolver, se deberá realizar el escalamiento respectivo al(los) fabricante(s). Para los casos reportados que ameriten ser escalados para que el servicio sea repuesto lo más pronto posible, CONTRATISTA realizará el seguimiento del caso e informará al BANCO enviando la siguiente información: Número de caso abierto, estado del caso reportado, responsable de la atención del caso.
- Las actualizaciones, parches, Fixes, microcódigo, firmware, release y cualquier otra característica de la solución deberán estar al día para evitar paralizaciones en la entrega del servicio. Es responsabilidad del Contratista informar al Banco las características y afectaciones posibles de las actualizaciones a ser implementadas para la revisión y autorización de su ejecución.
- Debe contar con el planeamiento de contingencia, donde se describa la forma como se despliega la configuración para la continuidad operatividad el cual debe estar incluido en el plan del trabajo, y ante algún cambio posterior deberá ser comunicado al Banco para su aprobación.
- El CONTRATISTA se encargará de monitorear la operatividad de toda la solución utilizando para ello los servicios contratados para ello. Este monitoreo debe garantizar la operatividad y buen funcionamiento de la solución de manera permanente durante la vigencia del contrato. Asimismo, deberá informar oportunamente al Banco de la Nación las incidencias que estén afectando o que potencialmente pudieran afectar la operatividad de la solución.
- El informe de remediación de incidentes deberá contener como mínimo los siguientes puntos:
  - Tipo de incidente, descripción, el tiempo de respuesta, el tiempo de solución, la solución aplicada, cumplimiento del SLA, el tiempo de retraso, este informe será evaluado por el Banco para su aprobación.
- El Contratista deberá informar al Banco inmediatamente sobre cambios en los lineamientos de atención, en:
  - Procedimientos de atención que no atenten los SLAs o vayan en contra de los requerimientos mínimos de las TDR
  - Escalamientos de incidentes
  - Direcciones electrónicas o teléfonos del personal que atenderá los incidentes
- El CONTRATISTA brindará los servicios profesionales directos del PSN, los mismos que serán atendidos por ingenieros de mantenimiento y soporte del PSN las 24 horas del día, los 7 días de la semana. Estas solicitudes serán atendidas a través de correo electrónico, chat o teléfono.

- El CONTRATISTA brindará el servicio de mantenimiento y soporte para la Banca Móvil y Banca por Internet según el tipo de incidencias que se puedan presentar en la etapa de producción.
- El PSN proveerá mantenimiento y soporte a un número ilimitado de casos de mantenimiento y soporte a través de un número ilimitado de contactos asignados.
- El PSN proveerá el mantenimiento y soporte necesario para mantener la operatividad de la nube, según el numeral 9.4 Prestación del Servicio de Nube a contratar.
- El CONTRATISTA brindará el mantenimiento y el soporte al Banco con la finalidad de optimizar el costo de los mismos y garantizar una arquitectura de nube adecuada.
- Dar orientación acerca de cómo se integran los servicios para satisfacer las necesidades del BANCO DE LA NACIÓN.
- Los términos del servicio de respuesta suministrados por el PSN deben ser los siguientes:
  - ✓ Asesoramiento general: < 24 horas
  - ✓ Atención por fallo en el sistema: < 12 horas
  - ✓ Atención por fallo en el sistema de producción: < 1 hora
  - ✓ Atención por Sistema de producción inactivo: < 30 Min
- El PSN proveerá niveles de soporte especializado para 1 evento al año planificado para mitigar riesgos y solución de problemas. El Banco podrá solicitar este tipo de servicio de manera adicional durante la ejecución del contrato.
- El PSN asignará un gerente técnico de cuenta para proporcionar orientación proactiva y coordinar el acceso a los programas y a los expertos.

14.2. Soporte Técnico para el Producto Implementado

El servicio técnico de mantenimiento permitirá al Banco dar respaldo tecnológico a la continuidad del servicio a implementar, asegurando la disponibilidad de los servicios de la Banca Móvil y la Banca por Internet. Este servicio no debe afectar a los tiempos de entrega previstos según el cronograma aprobado.

Este servicio iniciará una vez que se realice el pase a producción del MVP 1 y demás MVPs, y se extiende hasta la finalización del contrato del proyecto.

Asimismo, El Contratista será responsable de validar la adecuada instalación y configuración de su solución en los ambientes del Banco (Productivo y no productivo). El Banco coordinará previamente con el proveedor para que realice sus validaciones y conformidad de los cambios en el ambiente operativo (hardware, software base, base de datos, equipo de comunicaciones y otros) para asegurar el correcto funcionamiento de la solución y posibles afectaciones en el servicio.

14.3. Atención de Incidencias del Servicio

El tiempo de respuesta ante una incidencia, se define como el tiempo transcurrido entre el momento en que la entidad notifica la avería o si la avería es detectada internamente por el CONTRATISTA y el momento en que un técnico del servicio empieza a trabajar en la resolución del problema y además se realiza la primera comunicación con la entidad.

Cada incidencia estará asociada a un nivel de severidad descrito a continuación:

Tabla 14: Cuadro de Atención de Incidencias del Servicio

Nivel de incidente	Atención de incidentes	Solución del incidente	Tiempo de Entrega de Informe de Remediación
Crítica	=< 30 minutos	=< 1 hora	=< 10 días
Alta	=< 1 hora	=< 2 horas	=< 12 días
Media	=< 2 horas	=< 4 horas	=< 14 días
Baja	=< 4 horas	=< 24 horas	=< 16 días

Crítica: Incidente que genera afectación total y/o parcial a la operación del negocio que ponen en riesgo serio la operatividad del BANCO DE LA NACIÓN en la atención a sus clientes. Este tipo de incidente ha dejado inoperativo y tiene un alto impacto de compromiso en cualquier servicio (ambiente de producción).

Alta: Incidente que genera afectación de servicios de TI (ambiente de producción). Este tipo de incidente ha dejado inoperativo total o parcialmente algún servicio y/o aplicación.

Media: Incidente que pueda generar un nivel de afectación de alguno de los servicios brindados (ambientes de producción, certificación o desarrollo).

Baja: Incidente que tiene un bajo impacto en los ambientes de producción, certificación o desarrollo en las actividades del BANCO DE LA NACIÓN, pero debe ser tratado y/o mitigado en una ventana de mantenimiento programado.

14.4. Atención de Requerimientos

Se entiende como requerimiento a toda petición que implique gestión de cambios, Estas labores de "gestión de cambios" tendrán las siguientes características:

- El trabajo solicitado debe ser ejecutado por el personal con perfil indicado en la sección FUNCIONES DEL PERSONAL DEL CONTRATISTA.
- La duración de estas actividades no está acotada completamente, ya que dependen de la complejidad de la petición que el BANCO demande.

Tiempo de Respuesta para Requerimientos

El Tiempo de Respuesta para requerimientos se define como el lapso desde que la entidad realiza un pedido al Contratista hasta que el requerimiento es recepcionado. Posteriormente, el personal especializado se comunicará con la entidad para informar que el requerimiento ha sido recibido y será atendido de manera oportuna.

El CONTRATISTA deberá ofrecer para la atención de requerimientos en el servicio de nube el siguiente horario de atención:

Horarios de atención de lunes a viernes de 9:00am a 6:00pm
Modalidad 8 x 5 a la semana
Tiempo de respuesta: <= 2 horas

Así mismo, el soporte debe brindar la resolución de incidencias reportadas para el correcto funcionamiento de la plataforma Banca Web, Banca Móvil y Back office.

Mantenimiento de las soluciones debido a cambios en el entorno de producción, actualización de librerías, políticas de seguridad y/o actualizaciones de tiendas de aplicaciones.

15. PLAN DE TRABAJO

Dentro de los diez (10) días calendario de suscrito el contrato, el Contratista presentará un Plan de Trabajo, el cual será aprobado por áreas responsables en el lapso máximo de cinco (05) días calendario. En caso de presentarse observaciones al Contratista tendrá un plazo máximo de tres (03) días calendario para subsanar. La aprobación del plan de trabajo no libera al Contratista de su responsabilidad directa con respecto a la correcta culminación de la prestación en el plazo estipulado. Aprobado el plan de trabajo, el Contratista deberá desarrollarlo en la forma prevista con las consideraciones y/o ocurrencias que puedan presentarse como notificaciones de mantenimiento correctivo durante los preventivos. En este caso, el plan de trabajo es flexible de tener modificaciones durante el desarrollo de los servicios y en coordinación con el personal que designe las áreas responsables.

Este plan de trabajo deberá contener los detalles técnicos del despliegue de los ambientes de Desarrollo, Certificación y Producción. Para las pruebas funcionales de los MVP 1, 2 y 3 en producción, se realizarán con un grupo acotado de usuarios, este grupo será definido por el Banco.

Durante los MVP 1, 2 y 3 en producción, la Banca Móvil y la Banca por Internet coexistirán con las versiones actuales de las plataformas digitales del Banco. Para el pase a producción del MVP 4, el contratista deberá planificar el pase a producción masivo, es decir que, la nueva versión de las plataformas digitales del Banco de la Nación esté disponible para todos los clientes del Banco. En este proceso de pase a producción masivo, la versión anterior de la Banca Móvil y la

Banca por Internet se deshabilitarán previamente a fin de garantizar una única versión de las plataformas digitales del Banco.

El Contratista deberá presentar un Plan de Trabajo que incluya, como mínimo, el detalle de los siguientes ítems:

Tabla 15: Cuadro del Plan de Trabajo

Hito	Descripción
A	Mapa completo de la arquitectura en nube, instalación y configuración de la arquitectura tecnológica y de ciberseguridad (Implementación de la arquitectura)
B	MVP 1 Diseño, Desarrollo, Certificación, Producción, Documentación y Pentesting
C	MVP 2 Diseño, Desarrollo, Certificación, Producción, Documentación y Pentesting
D	MVP 3 Diseño, Desarrollo, Certificación, Producción, Documentación y Pentesting
E	MVP 4 Diseño, Desarrollo, Certificación, Producción, Documentación y Pentesting
F	Gestión de eventos e incidentes de seguridad informática
G	Fin del proyecto

15.1. Responsables de Aprobación

El responsable de la aprobación del informe funcional es:

- Subgerencia de Innovación Digital de la Gerencia de Banca Digital

Los responsables de la aprobación del informe técnico serán las siguientes áreas de la Gerencia de Tecnologías de la Información:

- Subgerencia de Construcción
- Subgerencia de Arquitectura
- Subgerencia de Producción
- Oficina de Seguridad Informática

15.2. Cronograma de Trabajo para el desarrollo de la Solución

El presente servicio tiene una vigencia de **420 días calendarios contados desde la aprobación del Plan de Trabajo**. Según se muestra en el siguiente cronograma:

Tabla 16: Cronograma de Trabajo para el desarrollo de la Solución

N°	Entregable	Referencia	Plazo máximo de ejecución (en días calendarios)	Inicio de la actividad
1	Análisis Funcional	7. ALCANCE Y DESCRIPCIÓN DEL SERVICIO	60	Desde el día siguiente de aprobado el Plan de Trabajo.
2	Diseño gráfico UX / UI	7. ALCANCE Y DESCRIPCIÓN DEL SERVICIO 7.1. Descripción y condiciones del servicio, literal "c".	75	Desde el día siguiente de aprobado el Plan de Trabajo.
3	Codificación y Pentesting MVP 1	7.2. Enrolamiento al canal digital 7.3. Enrolamiento a la Cuenta DNI 7.4 Afiliación a la Clave Dinámica Digital (CDD) 7.5 Gestión de Claves Centralizadas 7.6 Recuperación de la contraseña de Internet 7.7 Primer Inicio de Sesión 7.8 Inicio de Sesión del Cliente Recurrente 7.9 Factores de Autenticación y Seguridad del Cliente 7.10 Consultas de Productos, Saldos y Movimientos 7.11 Transferencias Bancarias 7.12 Retiro sin tarjeta y por agentes corresponsales 7.13 Módulo de Seguridad 7.14 Configuración de Multidioma (lenguas originarias)	105	Desde el día siguiente de aprobado el Análisis funcional
4	Despliegue en producción MVP 1	-	15	Desde el día siguiente de aprobado la Codificación y Pentesting MVP 1
5	Codificación y Pentesting MVP 2	7.15 Pago de Servicios y pago a empresas 7.16 Recargas móviles 7.11 Transferencias Bancarias (Diferidas) 7.17 Actualización de Datos	75	Desde el día siguiente de aprobado el Despliegue en producción MVP 1

		Personales 7.18 Operaciones Favoritas 7.19 Giros Nacionales 7.20 Bloqueo de Tarjetas de Débito o de Crédito		
6	Despliegue en producción MVP 2	-	15	Desde el día siguiente de aprobado la Codificación y Pentesting MVP 2
7	Codificación y Pentesting MVP 3	7.21 Pago de Tarjeta de Crédito 7.22 Créditos Digitales 7.23 Consulta de Estado de Cuenta 7.24 Ubicación de Agencias, Cajeros y Agentes 7.25 Configuración de los atributos de Cuentas y Tarjetas de los clientes	75	Desde el día siguiente de aprobado el Despliegue en producción MVP 2
8	Despliegue en producción MVP 3	-	15	Desde el día siguiente de aprobado la Codificación y Pentesting MVP 3
9	Codificación y Pentesting MVP 4	7.26 Módulo de Administración 7.27 Pago de Tasas	45	Desde el día siguiente de aprobado el Despliegue en producción MVP 3
10	Despliegue en producción MVP 4	-	15	Desde el día siguiente de aprobado la Codificación y Pentesting MVP 4

16. ENTREGABLES

16.1. Documentación remitida por el Contratista

El proveedor ganador de la buena pro deberá considerar los objetivos de la contratación, las actividades y alcance del servicio con la finalidad de atender

el requerimiento expresado en el presente documento, presentando los entregables exigidos en el Anexo 03 de la Directiva del Ciclo de Vida del Software BN-DIR-8300-147-02.

Luego de ser recibidos de manera formal y completa cada uno de los entregables solicitados, éstos deberán ser aprobados por las áreas correspondientes (ver Tabla 15: Cuadro de Aprobación por Área Responsable), en un plazo no mayor de diez (10) días calendario a partir de su recepción. De existir observaciones, se le otorgará a EL PROVEEDOR un plazo para subsanar no mayor de diez (10) días calendario.

Tanto los informes, así como los documentos exigidos deberán ser puestos a disposición del Banco de la Nación impresos y en medio magnético (CD, DVD o USB) en formato PDF y en idioma español.

Sin perjuicio a lo anterior, el Contratista deberá presentar con cada hito, el informe de la implementación de acuerdo al siguiente cuadro:

Tabla 17: Cuadro de Entregables para los Productos Mínimos Viables (MVP)

Nro.	Entregables para los Productos Mínimos Viables (MVP)
1	Los entregables deberán seguir los procesos de la "Metodología para el Ciclo de Vida del Software" (ver Anexo N° 9) 

En cumplimiento del numeral 34 Propiedad Intelectual (Derechos de autor) de los Términos de Referencia, el proveedor adjudicatario deberá entregar al Banco de la Nación, de forma exclusiva y sin restricciones, los siguientes recursos:

- **Códigos fuente:** Todos los códigos fuente desarrollados para la implementación de la nueva plataforma bancaria, incluyendo aplicaciones móviles, web y backend. Asimismo, el proveedor adjudicado deberá hacer entrega de los formatos o archivos editables utilizados en la etapa de análisis y diseño UX/UI.
- **Librerías de software:** Todas las librerías de software de terceros utilizadas en el desarrollo de la plataforma, junto con las licencias correspondientes que permitan su uso y modificación por parte del Banco de la Nación.
- **Documentación técnica:** Documentación completa y actualizada de la plataforma. El Contratista deberá elaborar estos documentos de acuerdo con los formatos estándares del Banco en cumplimiento de la Metodología del Ciclo de Vida de Software (Directiva BN-DIR-8300-

147-01), que será entregado a la firma del contrato. En caso de que el Banco y el proveedor acuerden la no aplicabilidad de un documento específico, el proveedor ganador del concurso deberá formalizar dicha decisión mediante un correo electrónico que detalle los motivos de la misma.

- **Otros recursos:** Cualquier otro recurso necesario para la instalación, configuración, operación y mantenimiento de la plataforma, como scripts de automatización, herramientas de desarrollo y archivos de configuración.

La entrega de estos recursos deberá realizarse de manera organizada y estructurada, en un formato que permita al personal técnico del Banco de la Nación comprender y utilizar los mismos sin dificultad. El objetivo es garantizar que el Banco pueda instalar y operar la plataforma de forma autónoma, sin depender del proveedor para futuras modificaciones o actualizaciones.
El proveedor deberá asegurar que los recursos entregados estén libres de cualquier restricción o dependencia que impida su uso y modificación por parte del Banco de la Nación. Esto incluye la eliminación de cualquier código ofuscado, licencias restrictivas o dependencias de software que no puedan ser adquiridas o utilizadas por el banco.

16.2. Conformidad de la Prestación

- Todos los entregables estarán sujetos a verificación y conformidad por parte del Banco de la Nación.
- El Acta de Conformidad del Servicio será dada por la Subgerencia Innovación Digital de la Gerencia de Banca Digital como área usuaria y con los informes favorables de las siguientes áreas:
  a. Informe de las pruebas funcionales de la Sección de Canales Virtuales de la Subgerencia de Canales Alternos de la Gerencia de Banca Digital.
  b. Informe emitido por la Gerencia de Tecnologías de Información que contenga los informes técnicos emitidos por la Subgerencia de Producción, de Construcción, de Arquitectura de TIC y por la Oficina de Seguridad Informática.
- Del punto anterior, los documentos serán remitidos a la Sección Ejecución y Seguimiento de Contratos de la Subgerencia de Compras y, comunicará vía correo electrónico al Contratista la emisión de dicho documento.
- La Conformidad y los respectivos informes de Tecnología y del área usuaria, deberán realizarse en un plazo que no excederá de los diez (10) días calendario de ser recibida la documentación correspondiente del Contratista.
- El Banco de la Nación podrá rechazar un Entregable solo si éste se hubiese desviado sustancialmente de los criterios de aceptación

acordados por escrito entre ambas partes, para ello el Banco de la Nación indicará mediante notificación escrita la naturaleza de dicha desviación.

- En caso se rechace, el Contratista rectificará cualquier diferencia identificada en el Entregable en un plazo no mayor de los siete (7) días calendario de ser recibida la notificación. Luego de la rectificación, el Entregable se deberá volver a presentar para su verificación posterior.
- El Contratista deberá presentar anualmente el informe de seguimiento el cual debe incluir como mínimo la siguiente documentación:

a. Informe de cumplimiento de Niveles de Servicio durante el ejercicio medido
b. Informe de número de cuentas activas durante el ejercicio medido.

- El Banco de la Nación tendrá la potestad de solicitar el cambio de cualquier miembro del Equipo de Trabajo del Contratista elegido, si este presenta deficiencias en su trabajo y/o faltas a la ética profesional.
- El Banco deberá otorgar una autorización expresa al Contratista, ya sea a través de un medio escrito o electrónico, para el paso a producción de los MPV del proyecto o en caso de lanzamiento de actualizaciones de los canales digitales.

17. TRANSFERENCIA DE CONOCIMIENTO

El Contratista deberá capacitar a los responsables de la administración tanto a nivel técnico como funcional en idioma español. Esta capacitación se realizará dentro del plazo de ejecución del servicio sin costo para el Banco de la Nación.
La transferencia de conocimiento solicitada será de manera presencial y/o remota, dentro del horario de oficina, para la cual el CONTRATISTA coordinará previamente con BANCO, las fechas y hora para su realización.

17.1. Capacitación Técnica

Se requiere capacitación especializada en la plataforma y las herramientas informáticas utilizadas por proveedor ganador de la buena pro para el personal técnico. La capacitación debe cubrir la configuración, administración y resolución de problemas de la plataforma, así como el uso eficiente de las herramientas automatizadas para optimizar los procesos y mejorar la productividad. Se espera que el proveedor ganador de la buena pro brinde esta capacitación de manera presencial y/o virtual, con material didáctico y ejercicios prácticos que permitan al personal técnico adquirir las habilidades necesarias para aprovechar al máximo la plataforma y las herramientas.
Se deberá considerar la transferencia de conocimiento de veinte (20) o la cantidad de colaboradores designados por EL BANCO, la misma que constará de un mínimo de ocho (8) horas y que deberán ser coordinados por la Gerencia de Tecnologías de Información y dentro de los noventa (90) días calendarios

como máximo contados a partir del día siguiente de la entrega de la **implementación de la infraestructura de producción**.

La transferencia de conocimiento será en el uso de la plataforma y/o herramientas, de ser el caso, que incluye:

- Servicio de Cómputo y Memoria
- Servicio de Almacenamiento
- Servicio de redes virtuales
- Servicio de balanceo de carga
- Servicio de base de datos relacionales y no relacionales
- Servicio de contenedores
- Servicio de VPN Site-to-site
- Servicio de DNS
- Servicios de integración y despliegue continuo
- Servicios de seguridad contratados

Las transferencias de conocimiento serán realizadas por personal propuesto por el CONTRASTISTA con certificación de arquitecto o similar como mínimo en la nube ofertada.

17.2. Capacitación Funcional

El Contratista deberá proporcionar capacitación a nivel funcional en un plazo máximo de 10 días calendarios, contados a partir del día siguiente a la entrega de la implementación del MVP 4 del pase masivo a producción**,** según el siguiente detalle:

Tabla 18: Cuadro de la Capacitación Funcional

Tipo de Capacitación	Sesión	Número de Sesiones	Número de horas
Funcional	Uso de registros de auditoría, gestión de accesos y políticas de seguridad	2	4
Funcional	Uso de la plataforma Back Office, traducción de contenidos, Plataforma de monitoreo y Reportes	2	4
	Total	4	8

La provisión de materiales y otros recursos necesarios para la capacitación será responsabilidad del Contratista. En el caso de que las capacitaciones se lleven a cabo en las instalaciones del Banco de la Nación, la entidad proporcionará las laptops o equipos de cómputo y el proyector.

Es importante destacar que la capacitación debe incorporar un enfoque basado en casos prácticos, con el objetivo de facilitar una comprensión más efectiva de los temas presentados.

Los horarios de la transferencia de conocimientos deberán estar programas de 8:30 a 17:30 horas, de lunes a viernes, en la oficina principal del Banco de la

Nación, ubicada en Av. Javier Prado Este 2499, en el distrito de San Borja.
Finalmente, el Banco estará facultado para registrar en video estas transferencias de conocimiento con el objetivo de abordar consultas futuras de manera eficiente.

18. GARANTÍA COMERCIAL

- **Alcance de la garantía:**

Contra defectos de diseño y/o desarrollo del software, disponibilidad o fallas de funcionamiento de los componentes alojados en la nube, entre otros supuestos ajenos al uso normal o habitual de los servicios y no detectables al momento que se otorgó la conformidad, sin perjuicio a la entidad.
Para el periodo de garantía, los recursos asignados por el Contratista deben ser totalmente independientes a los recursos asignados a los servicios de soporte y mejoras continuas.
Se considerarán como garantía todos los errores detectados durante la operación en producción, los cuales hayan sido originados por fallas en la etapa de construcción respecto de las definiciones realizadas, aun cuando estos procesos hayan sido aprobados por el Banco de la Nación en etapa de pruebas integrales.
Las mejoras por garantía consideran los mismos SLA's declarados.

- **Periodo de la garantía:**

La garantía debe incluir la corrección de cualquier error o diferencia con lo definido hasta 12 meses después de poner en producción masiva el último entregable correspondiente en el MVP 4.

- **Inicio del cómputo de la garantía:**

La garantía entrará en vigor después de poner en producción el último entregable, que corresponde al MVP 4.

19. LUGAR Y PLAZO DE LA PRESTACIÓN DEL SERVICIO

19.1. Lugar de la Prestación del Servicio

El servicio se ofrecerá en la sede principal del Banco de la Nación, ubicada en la Av. Javier Prado Este 2499, San Borja. El desarrollo del proyecto podrá ser realizado de forma remota. No obstante, el Banco tendrá la opción de solicitar presencialidad en caso lo considere necesario. Las actividades y las reuniones de trabajo con el personal del Banco se llevarán a cabo a través de la Plataforma Virtual del Banco o en la mencionada oficina principal.
El Banco dispondrá de los puestos de trabajo según disponibilidad de espacios, que no incluyen equipos tecnológicos para el desarrollo de la solución. En caso de necesitar conexión a internet u otros accesos especiales deberán ser coordinados previamente con el Gerente del Proyecto y la Sección de Seguridad del Banco.
La jornada laboral en el Banco de la Nación es de cinco (05) días a la

semana, en horario de 08:30 a 17:30. No obstante, el Banco podrá coordinar con el proveedor los horarios especiales o fuera del horario indicado, cuando el Proyecto lo requiera, para garantizar el cumplimiento de los plazos establecidos en la ejecución del servicio.

En caso de que el Contratista necesite acceder a las instalaciones del Banco de la Nación, deberá comunicarse con el coordinador designado por el Banco para obtener la autorización correspondiente. El ingreso a dichas instalaciones estará sujeto al cumplimiento de los protocolos establecidos por el área correspondiente del Banco de la Nación por parte del Contratista de servicios.

Los equipos de cómputo y programas de seguridad, como antivirus y firewall, necesarios para el servicio, deberán ser proporcionados por el proveedor en el caso del trabajo remoto. En cuanto al trabajo presencial o remoto, el Banco facilitará las conexiones VPN para los equipos de cómputo correspondientes del proveedor, sujeto a coordinación previa con el responsable designado por la institución.

19.2. Plazo de Ejecución de la Prestación del Servicio

Desarrollo de la Aplicación

El plazo de contratación del servicio de la nueva plataforma bancaria para los canales digitales Banca Móvil y Banca por Internet del Banco de la Nación será de **420 días calendarios**. El inicio de la contraprestación del servicio será a partir del día siguiente de aprobado el **Plan de Trabajo**.

Servicios de Nube

El plazo de contratación de lo servicio de nube para la nueva plataforma bancaria para los canales digitales Banca Móvil y Banca por Internet del Banco de la Nación será de **36 meses** como máximo. El inicio de la contraprestación del servicio será a partir del día siguiente de aprobado el **Plan de Trabajo**.

19.3. Servicio de Asistencia para Alcanzar la Mejora Continua de la Solución

El servicio de Mejora Continua (ver numeral 33. Mejora Continua del Servicio) tendrá una duración de **90 días calendarios** bajo la modalidad de bolsa de trabajo que considera 600 horas mensuales (total del servicio 1,800 horas), terminado el periodo de 90 días, el servicio tendrá la modalidad a demanda durante el tiempo de ejecución del contrato.

El inicio del servicio de Mejora Continua empezará al día siguiente de la suscripción del Acta de Conformidad correspondiente al MVP 4.

20. OBLIGACIONES DEL CONTRATISTA

1. Cumplir con las obligaciones derivadas de este servicio, así como con las normativas y directrices internas vigentes del Banco de la Nación aplicables a esta modalidad contractual.
2. Realizar las actividades contractuales en las fechas acordadas.
3. Aceptar la supervisión de la ejecución del servicio por parte del Banco de la Nación.
4. Mantener la confidencialidad de la información proporcionada por el Banco de la Nación para la prestación del servicio, sin divulgar, revelar, entregar o poner a disposición de terceros, ya sea en o fuera del lugar de trabajo, a menos que cuente con una autorización expresa del Banco de la Nación. El incumplimiento de esta obligación de confidencialidad, especialmente en lo que respecta a datos personales, facultará al Banco de la Nación para resolver el contrato de acuerdo a los procedimientos y normativas establecidas.
5. Abstenerse de llevar a cabo acciones u omisiones que puedan perjudicar la imagen institucional del Banco de la Nación, manteniendo la confidencialidad en todo momento.
6. Implementar medidas de seguridad para garantizar la integridad de la documentación proporcionada.
7. Asegurar que toda la tecnología y los programas del sistema cumplan con todas las condiciones técnicas establecidas y se ajusten por completo a los requisitos de aceptación especificados.

20.1. Metodología de Implementación

El Contratista debe asegurar una gestión eficiente del proyecto, utilizando una metodología de gestión de proyectos validada y reconocida a nivel internacional. Además, deberá manejar la documentación de manera apropiada, estableciendo juntamente con el Banco de la Nación mecanismos de control, avances y entregables periódicos de acuerdo al plan de trabajo establecido.

El proveedor debe demostrar y asignar personal al proyecto que tenga experiencia comprobada en este tipo de metodologías. Además, debe contar con herramientas que automatizan y garantizan la integración y el despliegue continuo entre cada MVP.

20.2. Plan de Comunicación e Informes

- El Contratista y su equipo deberán participar en sesiones de seguimiento diario del proyecto, conocidas como reuniones de coordinación, así como entregar informes y asistir a reuniones semanales para medir el avance y revisar el estado del avance.

- Entregar informes ejecutivos de forma quincenal sobre el estado del proyecto para su revisión por parte del comité ejecutivo del proyecto o al equipo que el Banco designe.
- Las plantillas para utilizar y las personas que participarán en las reuniones acordadas serán definidas de común acuerdo entre el Contratista y los responsables de la gestión del proyecto del Banco de la Nación.

21. FORMA DE PAGO

El pago se realizará en la moneda nacional (soles) por la prestación efectiva del servicio instalado. En el caso de ofertas presentadas en moneda extranjera, el pago se ajustará al tipo de cambio Venta Promedio Ponderado, publicado por la Superintendencia de Banca y Seguros (SBS) en la fecha del registro contable de los pagos. Este proceso se llevará a cabo luego de recibir de manera formal y completa toda la documentación correspondiente.

El Contratista debe incluir en su propuesta los rangos de uso mensual correspondientes a los distintos componentes de la solución. Esto implica detallar la capacidad de la solución para manejar distintos volúmenes de transacciones, especificando claramente los límites de uso para cada componente, como el almacenamiento en la nube, el procesamiento de datos, la transferencia de datos y otros servicios relacionados. Es fundamental que los rangos de uso sean adecuados, por precio unitario según el rango mensual y estén alineados con las necesidades del proyecto, permitiendo una planificación precisa y garantizando la escalabilidad de la solución a lo largo del tiempo. En este contexto, el Contratista deberá considerar el Anexo N° 6 para la presentación de sus rangos de uso propuestos, el cual deberá ser incluido en su propuesta económica.

El contratista deberá consolidar la documentación correspondiente según el siguiente cuadro:

Tabla 19: Cuadro de Aprobación por Área Responsable

Gerencia o Subgerencia Responsable	Referencia
Gerencia de Banca Digital (Subgerencia Innovación Digital)	Numeral 21.1. Diseño, Desarrollo e Implementación de la Solución
Gerencia de Tecnologías de la Información	Numeral 21.2. Servicios de alojamiento, procesamiento y seguridad de la Solución
Gerencia de Banca Digital (Subgerencia Innovación Digital)	Numeral 21.3 Componente opcional – Cuenta DNI
Gerencia de Banca Digital (Subgerencia Innovación Digital)	Numeral 21.4 19.3. Servicio de Asistencia para Alcanzar la Mejora Continua de la Solución

La documentación necesaria para los pagos por parte del Contratista deberá ser enviada en formato físico a la sede central del Banco de la Nación, ubicada en la calle Arqueología N° 120, San Borja, Lima, durante el horario de oficina.

21.1. Diseño, Desarrollo e Implementación de la Solución

El pago se realizará tras la emisión del Acta de Conformidad correspondiente a cada entregable definido.

El Banco realizará los pagos al Contratista en diez (10) partes, según se especifica en el cuadro de plazos de los entregables y porcentajes de pago correspondiente al desarrollo de la solución. Estos pagos estarán condicionados al cumplimiento del envío de los documentos establecidos en el numeral 16 de Entregables.

A fin de proceder con el pago correspondiente al entregables, el Contratista deberá remitir al Banco de la Nación la siguiente documentación:

e. Carta simple dirigida al Subgerente de Compras de la Gerencia de Administración y Logística.
f. Comprobante de pago
g. Acta de Conformidad original de la Subgerencia de Innovación Digital como área usuaria
h. Informe de la Subgerencia de Innovación Digital como área usuaria y sus anexos, en caso de que los haya.

El Contratista estará encargado de desarrollar e implementar los APIs necesarios para el proyecto (ver numeral 13. Desarrollo de APIs). El costo de estos APIs debe estar incluido en los costos totales de desarrollo e implementación de la nueva plataforma de los Canales Digitales del Banco de Nación y no será sujeto a pagos diferenciados.

Para reflejar la importancia y el peso de las actividades para cada MVP, se asignará un porcentaje de la facturación total de desarrollo de la solución, basado en la complejidad y el valor de las funcionalidades a desarrollar.

Los pagos se realizarán en base a los entregables propuestos, según el siguiente cuadro:

Tabla 20: Forma de Pago para el Desarrollo e Implementación del Producto.

N°	Entregable	Referencia	Días calendarios del plazo de entregables, contados desde aprobación del Plan de Trabajo	Porcentaje de Facturación por Desarrollo de Solución
1	Análisis funcional	7. ALCANCE Y DESCRIPCIÓN DEL SERVICIO	60	5.00%
2	Diseño UX / UI	7. ALCANCE Y DESCRIPCIÓN DEL SERVICIO 7.1. Descripción y condiciones del servicio, literal "c".	75	5.00%
3	Codificación y Pentesting MVP 1	7.2. Enrolamiento al canal digital 7.3. Enrolamiento a la Cuenta DNI 7.4 Afiliación a la Clave Dinámica Digital (CDD) 7.5 Gestión de Claves	165	11.00%

		Centralizadas 7.6 Recuperación de la contraseña de Internet 7.7 Primer Inicio de Sesión 7.8 Inicio de Sesión del Cliente Recurrente 7.9 Factores de Autenticación y Seguridad del Cliente 7.10 Consultas de Productos, Saldos y Movimientos 7.11 Transferencias Bancarias 7.12 Retiro sin tarjeta y por agentes corresponsales 7.13 Módulo de Seguridad 7.14 Configuración de Multidioma (lenguas originarias)		
4	Despliegue en Producción MVP 1	-	180	14.50%
5	Codificación y Pentesting MVP 2	7.15 Pago de Servicios y pago a empresas 7.16 Recargas móviles 7.11 Transferencias Bancarias (Diferidas) 7.17 Actualización de Datos Personales 7.18 Operaciones Favoritas 7.19 Giros Nacionales 7.20 Bloqueo de Tarjetas de Débito o de Crédito	255	9.00%
6	Despliegue en Producción MVP 2	-	270	13.50%
7	Codificación y Pentesting MVP 3	7.21 Pago de Tarjeta de Crédito 7.22 Créditos Digitales 7.23 Consulta de Estado de Cuenta 7.24 Ubicación de Agencias, Cajeros y Agentes 7.25 Configuración de los atributos de Cuentas y Tarjetas de los clientes	345	9.00%

8	Despliegue en Producción MVP 3	-	360	13.50%
9	Codificación y Pentesting MVP 4	7.26 Módulo de Administración 7.27 Pago de Tasas	405	9.00%
10	Despliegue en Producción MVP 4	-	420	10.50%
			Total	**100.00%**

El proveedor ganador de la buena pro deberá cumplir con los porcentajes y plazos establecidos en la Tabla 16 Forma de Pago para el Desarrollo e Implementación del Producto para los entregables 1 (Análisis Funcional) y 2 (Diseño UX/UI), independientemente de si opta por ejecutar estas actividades en su totalidad al inicio del proyecto o de forma parcial y proporcional en cada MVP (Producto Mínimo Viable).

21.2. Servicios de Alojamiento, Procesamiento y Seguridad de la Solución

Los pagos se efectuarán por prestaciones completadas de acuerdo a las tarifas establecidas para cada rango según modalidad de validación y los consumos mensuales de prestaciones efectivas y debidamente acreditadas según los requisitos solicitados.

b. Forma y Plazo para el Pago del Servicio de Alojamiento, Procesamiento y Seguridad

Los pagos se realizarán en base a la implementación de los hitos propuestos, según el siguiente cuadro:

Tabla 21: Forma de pago para los costos fijos el Servicio de Alojamiento, Procesamiento y Seguridad de la Solución

Implementación del servicio de nube	Hitos	Referencias	Plazo máximo de entrega (en días calendarios)	% de pago
Para el pago de la implementación de la infraestructura	Despliegue Base para los Ambientes	21.2 Servicios de Alojamiento, Procesamiento y Seguridad de la Solución, literal b.1 Para el Pago de la Implementación de la Infraestructura, literal b.1.1	55 días posteriores a la fecha de la firma del acta de conformidad del plan de trabajo.	25% del costo de implementación de la infraestructura

		Despliegue Base para los Ambientes		
	Despliegue del Ambiente de Desarrollo (DEV)	21.2 Servicios de Alojamiento, Procesamiento y Seguridad de la Solución, literal b.1 Para el Pago de la Implementación de la Infraestructura, b.1.2 Despliegue del Ambiente de Desarrollo (DEV)	35 días posteriores a la fecha de aprobación del informe técnico de Despliegue base para los ambientes.	25% del costo de implementación de la infraestructura
	Despliegue del Ambiente de Calidad (QA)	21.2 Servicios de Alojamiento, Procesamiento y Seguridad de la Solución, literal b.1 Para el Pago de la Implementación de la Infraestructura, b.1.3 Despliegue del Ambiente de Calidad (QA)	35 días posteriores a la fecha de aprobación del informe técnico de Despliegue del ambiente de desarrollo.	25% del costo de implementación de la infraestructura
	Despliegue del Ambiente de Producción (PRD)	21.2 Servicios de Alojamiento, Procesamiento y Seguridad de la Solución, literal b.1 Para el Pago de la Implementación de la Infraestructura, b.1.4 Despliegue del Ambiente de Producción (PRD)	35 días posteriores a la fecha de aprobación del informe técnico de Despliegue del ambiente de calidad.	25% del costo de implementación de la infraestructura
Para el pago de la implementación del ambiente	Servicio de Implementación Plataforma de Protección	21.2 Servicios de Alojamiento, Procesamiento y	60 días posteriores a la fecha del informe de aprobación del ambiente de	25% del costo de implementación del ambiente de seguridad

de seguridad	para Aplicaciones CNAPP	Seguridad de la Solución, literal b.2 Para el Pago de la Implementación del Ambiente de Seguridad, b.2.1 Servicio de Implementación Plataforma de Protección para Aplicaciones CNAPP	desarrollo (DEV).	
	Servicio Implementación Firewall	21.2 Servicios de Alojamiento, Procesamiento y Seguridad de la Solución, literal b.2 Para el Pago de la Implementación del Ambiente de Seguridad, b.2.2 Servicio Implementación Firewall		25% del costo de implementación del ambiente de seguridad
	Servicio Implementación SaaS de Seguridad para los servicios WAF, ataques volumétricos de denegación de servicio y servicio de seguridad de API Discovery	21.2 Servicios de Alojamiento, Procesamiento y Seguridad de la Solución, literal b.2 Para el Pago de la Implementación del Ambiente de Seguridad, b.2.3 Servicio Implementación SaaS de Seguridad para los Servicios WAF, Ataques Volumétricos de Denegación de Servicio y Servicio de Seguridad de API Discovery		25% del costo de implementación del ambiente de seguridad

	Servicio Implementación para el Servicio de Detección Avanzada para ataques de Bots Automatizados	21.2 Servicios de Alojamiento, Procesamiento y Seguridad de la Solución, literal b.2 Para el Pago de la Implementación del Ambiente de Seguridad, b.2.4 Servicio Implementación para el Servicio de Detección Avanzada para Ataques de Bots Automatizados		25% del costo de implementación del ambiente de seguridad

Tabla 22: Forma de pago para los costos variables el Servicio de Alojamiento, Procesamiento y Seguridad de la Solución

Implementación del servicio de nube	Hitos	Referencias	Plazo máximo de entrega (en días calendarios)
Para el pago mensual* por uso de infraestructura y ambiente de seguridad	Pago mensual de infraestructura	21.2 Servicios de Alojamiento, Procesamiento y Seguridad de la Solución, literal b.3 Para el Pago Mensual por Uso de Infraestructura y Ambiente de Seguridad, b.3.1 Pago Mensual de Infraestructura	El pago por el uso de los componentes de infraestructura se realizará al final de cada mes según los consumos realizados por cada uno de estos componentes especificados en las Tablas de Capacidades. (considerar DEV, QA, PRD, seguridad y compartidos).
	Pago mensual del servicio de seguridad	21.2 Servicios de Alojamiento, Procesamiento y Seguridad de la Solución, literal b.3 Para el Pago Mensual por Uso de Infraestructura y Ambiente de Seguridad, b.3.2 Pago Mensual del Servicio de Seguridad	
Para el pago del soporte técnico	Pago mensual por soporte técnico	21.2 Servicios de Alojamiento, Procesamiento y Seguridad de la Solución, literal b.4 Para el Pago del Soporte Técnico, b.4.1 Pago Mensual de Soporte Técnico	El pago por el soporte y mantenimiento de la infraestructura y seguridad se realizará al final de cada mes, hasta el final del contrato, iniciándose este soporte y mantenimiento al finalizar la

			implementación del ambiente de producción

*El pago se realizará de acuerdo con el consumo efectivo mensual y las tarifas por rangos y componentes del servicio que presenten los postores en su oferta económica.

b.1 Para el Pago de la Implementación de la Infraestructura

La documentación para los pagos por parte del Contratista será remitida en formato físico a la sede central del Banco de la Nación, sitio en calle Arqueología N° 120, San Borja, Lima, en horario de oficina.

b.1.1 Despliegue Base para los Ambientes

El Contratista deberá entregar un informe que evidencie el despliegue base de servicios y configuraciones para los ambientes a implementar (Desarrollo, Certificación y Producción), así como la descripción de cada uno de los componentes a ser desplegados en esta etapa y si hubiera alguna descripción adicional también debe ser informada.

El Banco revisará el informe como máximo en 5 días calendario como máximo y si hubiera alguna observación se le indicará al Contratista a través de correo electrónico al líder de proyecto del Contratista para la subsanación respectiva, para lo cual el Contratista tendrá 5 días calendarios adicionales como máximo para la subsanación. Una vez concluida la revisión por parte del Banco se emitirá un informe técnico y posteriormente el acta de conformidad para el pago.

Los responsables de la aprobación del informe técnico serán las áreas siguientes:

- Subgerencia de Construcción
- Subgerencia de Arquitectura
- Subgerencia de Producción
- Oficina de Seguridad informática

El Banco comunicara al Contratista la fecha de aprobación del informe técnico para que al día siguiente inicie la implementación del ambiente de desarrollo.

El responsable del acta de conformidad será la Subgerencia de Innovación Digital de la Gerencia Banca Digital.

Los documentos a entregar por parte del Contratista para el pago serán:

- Carta simple dirigida al subgerente de compras de la gerencia de administración y logística
- Acta de conformidad suscrita por la Subgerencia de Innovación Digital de la Gerencia Banca Digital.
- Comprobante de pago.
- Informe técnico por parte de la Gerencia de TI especificado anteriormente.
- Copia del contrato.

b.1.2 Despliegue del Ambiente de Desarrollo (DEV)

El Contratista deberá entregar un informe que evidencie el despliegue de los componentes necesarios para el uso del ambiente de desarrollo, así como la habilitación de servicios y configuraciones necesarias, así como la descripción de cada uno de los componentes y servicios desplegados en esta etapa y si hubiera alguna descripción adicional también debe ser informada.
El Banco revisará el informe como máximo en 5 días calendario y si hubiera alguna observación se le indicará al Contratista a través de correo electrónico al líder de proyecto del Contratista para la subsanación respectiva, para lo cual el Contratista tendrá 5 días calendarios adicionales como máximo para la subsanación. Una vez concluida la revisión por parte del Banco se emitirá un informe técnico y posteriormente el acta de conformidad para el pago.
Los responsables de la aprobación del informe técnico serán las áreas siguientes es:

- Subgerencia de Construcción
- Subgerencia de Arquitectura
- Subgerencia de Producción
- Oficina de Seguridad Informática

El Banco comunicara al Contratista la fecha de aprobación del informe técnico para que al día siguiente inicie la implementación del ambiente de Calidad.
El responsable del acta de conformidad será la Subgerencia de Innovación Digital de la Gerencia Banca Digital.
Los documentos a entregar por parte del Contratista para el pago serán:

- Carta simple dirigida al subgerente de compras de la gerencia de administración y logística
- Acta de conformidad suscrita por la Subgerencia de Innovación Digital de la Gerencia Banca Digital.
- Comprobante de pago.

- Informe técnico por parte de la Gerencia de TI especificado anteriormente.
- Copia del contrato.

b.1.3 Despliegue del Ambiente de Calidad (QA)

El Contratista deberá entregar un informe que evidencie el despliegue de los componentes necesarios para el uso del ambiente de calidad, así como la habilitación de servicios y configuraciones necesarias, así como la descripción de cada uno de los componentes y servicios desplegados en esta etapa y si hubiera alguna descripción adicional también debe ser informada.
El Banco revisará el informe como máximo en 5 días calendario y si hubiera alguna observación se le indicará al Contratista a través de correo electrónico al líder de proyecto del Contratista para la subsanación respectiva, para lo cual el Contratista tendrá 5 días calendarios adicionales como máximo para la subsanación. Una vez concluida la revisión por parte del Banco se emitirá un informe técnico y posteriormente el acta de conformidad para el pago.
Los responsables de la aprobación del informe técnico serán las áreas siguientes es:

- Subgerencia de Construcción
- Subgerencia de Arquitectura
- Subgerencia de Producción
- Oficina de Seguridad Informática

El Banco comunicara al Contratista la fecha de aprobación del informe técnico para que al día siguiente inicie la implementación del ambiente de Producción.
El responsable del acta de conformidad será la Subgerencia de Innovación Digital de la Gerencia Banca Digital.
Los documentos a entregar por parte del Contratista para el pago serán:

- Carta simple dirigida al subgerente de compras de la gerencia de administración y logística
- Acta de conformidad suscrita por la Subgerencia de Innovación Digital de la Gerencia Banca Digital.
- Comprobante de pago.
- Informe técnico por parte de la Gerencia de TI especificado anteriormente.
- Copia del contrato.

b.1.4 Despliegue del Ambiente de Producción (PRD)

El Contratista deberá entregar un informe que evidencie el despliegue de los componentes necesarios para el uso del

ambiente de producción, así como la habilitación de servicios y configuraciones necesarias, así como la descripción de cada uno de los componentes y servicios desplegados en esta etapa y si hubiera alguna descripción adicional también debe ser informada.
El Banco revisará el informe como máximo en 5 días calendario y si hubiera alguna observación se le indicará al Contratista a través de correo electrónico al líder de proyecto del Contratista para la subsanación respectiva, para lo cual el Contratista tendrá 5 días calendarios adicionales como máximo para la subsanación. Una vez concluida la revisión por parte del Banco se emitirá un informe técnico y posteriormente el acta de conformidad para el pago.
Los responsables de la aprobación del informe técnico serán las áreas siguientes es:

- Subgerencia de Construcción
- Subgerencia de Arquitectura
- Subgerencia de Producción
- Oficina de Seguridad Informática

El responsable del acta de conformidad será la Subgerencia de Innovación Digital de la Gerencia Banca Digital.
Los documentos a entregar por parte del Contratista para el pago serán:

- Carta simple dirigida al subgerente de compras de la gerencia de administración y logística
- Acta de conformidad suscrita por la Subgerencia de Innovación Digital de la Gerencia Banca Digital.
- Comprobante de pago.
- Informe técnico por parte de la Gerencia de TI especificado anteriormente.
- Copia del contrato.

b.2 Para el Pago de la Implementación del Ambiente de Seguridad

b.2.1 Servicio de Implementación Plataforma de Protección para Aplicaciones CNAPP

El Contratista deberá entregar un informe sobre el despliegue de los componentes necesarios para el uso de la plataforma de protección para aplicaciones (CNAPP), así como la habilitación de servicios y configuraciones necesarias, así como la descripción de cada uno de los componentes y servicios desplegados en esta etapa y si hubiera alguna descripción adicional también debe ser informada.
El Banco revisará el informe como máximo en 5 días calendario y si hubiera alguna observación se le indicará al Contratista a través de correo electrónico al líder de proyecto del Contratista para la subsanación respectiva, para lo cual el Contratista tendrá 5 días calendarios adicionales como máximo para la subsanación. Una

vez concluida la revisión por parte del Banco se emitirá un informe técnico y posteriormente el acta de conformidad para el pago.
Los responsables de la aprobación del informe técnico serán las áreas siguientes es:

- Subgerencia de Construcción
- Subgerencia de Arquitectura
- Subgerencia de Producción
- Oficina de Seguridad Informática

El responsable del acta de conformidad será la Subgerencia de Innovación Digital de la Gerencia Banca Digital.
Los documentos a entregar por parte del Contratista para el pago serán:

- Carta simple dirigida al subgerente de compras de la gerencia de administración y logística
- Acta de conformidad suscrita por la Subgerencia de Innovación Digital de la Gerencia Banca Digital.
- Comprobante de pago.
- Informe técnico por parte de la Gerencia de TI especificado anteriormente.
- Copia del contrato.

b.2.2 Servicio Implementación Firewall

El Contratista deberá entregar un informe sobre el despliegue de los componentes necesarios para el uso de los servicios de Firewall, así como la habilitación de servicios y configuraciones necesarias, así como la descripción de cada uno de los componentes y servicios desplegados en esta etapa y si hubiera alguna descripción adicional también debe ser informada.
El Banco revisará el informe como máximo en 5 días calendario y si hubiera alguna observación se le indicará al Contratista a través de correo electrónico al líder de proyecto del Contratista para la subsanación respectiva, para lo cual el Contratista tendrá 5 días calendarios adicionales como máximo para la subsanación. Una vez concluida la revisión por parte del Banco se emitirá un informe técnico y posteriormente el acta de conformidad para el pago.
Los responsables de la aprobación del informe técnico serán las áreas siguientes es:

- Subgerencia de Construcción
- Subgerencia de Arquitectura
- Subgerencia de Producción
- Oficina de Seguridad Informática

El responsable del acta de conformidad será la Subgerencia de Innovación Digital de la Gerencia Banca Digital.

Los documentos a entregar por parte del Contratista para el pago serán:

- Carta simple dirigida al subgerente de compras de la gerencia de administración y logística
- Acta de conformidad suscrita por la Subgerencia de Innovación Digital de la Gerencia Banca Digital.
- Comprobante de pago.
- Informe técnico por parte de la Gerencia de TI especificado anteriormente.
- Copia del contrato.

b.2.3 Servicio Implementación SaaS de Seguridad para los Servicios WAF, Ataques Volumétricos de Denegación de Servicio y Servicio de Seguridad de API Discovery

El Contratista deberá entregar un informe sobre el despliegue de los componentes necesarios para el uso de los Servicio Implementación SaaS de Seguridad para los servicios WAF, ataques volumétricos de denegación de servicio y servicio de seguridad de API Discovery, así como la habilitación de servicios y configuraciones necesarias, así como la descripción de cada uno de los componentes y servicios desplegados en esta etapa y si hubiera alguna descripción adicional también debe ser informada.

El Banco revisará el informe como máximo en 5 días calendario y si hubiera alguna observación se le indicará al Contratista a través de correo electrónico al líder de proyecto del Contratista para la subsanación respectiva, para lo cual el Contratista tendrá 5 días calendarios adicionales como máximo para la subsanación. Una vez concluida la revisión por parte del Banco se emitirá un informe técnico y posteriormente el acta de conformidad para el pago.

Los responsables de la aprobación del informe técnico serán las áreas siguientes es:

- Subgerencia de Construcción
- Subgerencia de Arquitectura
- Subgerencia de Producción
- Oficina de Seguridad Informática

El responsable del acta de conformidad será la Subgerencia de Innovación Digital de la Gerencia Banca Digital.

Los documentos a entregar por parte del Contratista para

el pago serán:

- Carta simple dirigida al subgerente de compras de la gerencia de administración y logística
- Acta de conformidad suscrita por la Subgerencia de Innovación Digital de la Gerencia Banca Digital.
- Comprobante de pago.
- Informe técnico por parte de la Gerencia de TI especificado anteriormente.
- Copia del contrato.

b.2.4 Servicio Implementación para el Servicio de Detección Avanzada para Ataques de Bots Automatizados

El Contratista deberá entregar un informe sobre despliegue de los componentes necesarios para el uso de los Servicio Implementación para el Servicio de Detección Avanzada para ataques de Bots Automatizados, así como la habilitación de servicios y configuraciones necesarias, así como la descripción de cada uno de los componentes y servicios desplegados en esta etapa y si hubiera alguna descripción adicional también debe ser informada.

El Banco revisará el informe como máximo en 5 días calendario y si hubiera alguna observación se le indicará al Contratista a través de correo electrónico al líder de proyecto del Contratista para la subsanación respectiva, para lo cual el Contratista tendrá 5 días calendarios adicionales como máximo para la subsanación. Una vez concluida la revisión por parte del Banco se emitirá un informe técnico y posteriormente el acta de conformidad para el pago.

Los responsables de la aprobación del informe técnico serán las áreas siguientes es:

- Subgerencia de Construcción
- Subgerencia de Arquitectura
- Subgerencia de Producción
- Oficina de Seguridad Informática

El responsable del acta de conformidad será la Subgerencia de Innovación Digital de la Gerencia Banca Digital.

Los documentos a entregar por parte del Contratista para el pago serán:

- Carta simple dirigida al subgerente de compras de la gerencia de administración y logística
- Acta de conformidad suscrita por la Subgerencia de Innovación Digital de la Gerencia Banca Digital.
- Comprobante de pago.
- Informe técnico por parte de la Gerencia de TI especificado anteriormente.

- Copia del contrato

b.3 Para el Pago Mensual por Uso de Infraestructura y Ambiente de Seguridad

b.3.1 Pago Mensual de Infraestructura

El pago por el uso de los componentes de infraestructura se realizará al final de cada mes según los consumos realizados por cada uno de estos componentes especificados en las Tablas de Capacidades. (considerar dev, qa, prd y compartidos).

En situaciones donde el servicio se inicie en un día que no coincida con el comienzo de un mes calendario, se aplicara el prorrateo. El prorrateo consistirá en calcular la proporción del servicio utilizado desde la fecha de inicio hasta el final del mes en curso y facturar únicamente por ese período inicial de manera proporcional.

El Contratista emitirá un informe a cada fin de mes indicando los consumos realizados por cada uno de los componentes, reportes de monitoreo, Incidencias generadas, así como las soluciones realizadas, además de recomendaciones de mejora de ser el caso.

El Banco revisará el informe como máximo en 5 días calendario y si hubiera alguna observación se le indicará al Contratista a través de correo electrónico al líder de proyecto del Contratista para la subsanación respectiva, para lo cual el Contratista tendrá 5 días calendarios adicionales como máximo para la subsanación. Una vez concluida la revisión por parte del Banco se emitirá un informe técnico y posteriormente el acta de conformidad para el pago.

Los responsables de la aprobación del informe técnico serán las áreas siguientes es:

- Subgerencia de Construcción
- Subgerencia de Producción

El responsable del acta de conformidad será la Subgerencia de Innovación Digital de la Gerencia Banca Digital.

Los documentos a entregar por parte del Contratista para el pago serán:

- Carta simple dirigida al subgerente de compras de la gerencia de administración y logística
- Acta de conformidad suscrita por la Subgerencia de Innovación Digital de la Gerencia Banca Digital.
- Comprobante de pago.
- Informe técnico por parte de la Gerencia de TI especificado anteriormente.
- Copia del contrato.

b.3.2 Pago Mensual del Servicio de Seguridad

El pago por el uso de los componentes de infraestructura se realizará al final de cada mes según los consumos realizados por cada uno de estos componentes especificado en la tabla de la sección 11.8. Especificaciones de capacidades de los servicios de seguridad. (considerar dev, qa, prd) y compartidos.
En situaciones donde el servicio se inicie en un día que no coincida con el comienzo de un mes calendario, se aplicara el prorrateo. El prorrateo consistirá en calcular la proporción del servicio utilizado desde la fecha de inicio hasta el final del mes en curso y facturar únicamente por ese período inicial de manera proporcional.
El Contratista emitirá un informe a cada fin de mes indicando los consumos realizados por cada uno de los componentes, reportes de monitoreo, Incidencias generadas, así como las soluciones realizadas, además de recomendaciones de mejora de ser el caso.
El Banco revisará el informe como máximo en 5 días calendario y si hubiera alguna observación se le indicará al Contratista a través de correo electrónico al líder de proyecto del Contratista para la subsanación respectiva, para lo cual el Contratista tendrá 5 días calendarios adicionales como máximo para la subsanación. Una vez concluida la revisión por parte del Banco se emitirá un informe técnico y posteriormente el acta de conformidad para el pago.
El responsable de la aprobación del informe técnico será el área siguiente:

- Oficina de Seguridad Informática

El responsable del acta de conformidad será la Subgerencia de Innovación Digital de la Gerencia Banca Digital.
Los documentos a entregar por parte del Contratista para el pago serán:

- Carta simple dirigida al subgerente de compras de la gerencia de administración y logística
- Acta de conformidad suscrita por la Subgerencia de Innovación Digital de la Gerencia Banca Digital.
- Comprobante de pago.
- Informe técnico por parte de la Gerencia de TI especificado anteriormente.
- Copia del contrato.

b.4 Para el Pago del Soporte Técnico

b.4.1 Pago Mensual de Soporte Técnico

El pago por el soporte y mantenimiento de la infraestructura y seguridad se realizará al final de cada mes, hasta el final del contrato, iniciándose este soporte y mantenimiento al finalizar la implementación del ambiente de producción como indicará el informe técnico de aprobación del ambiente de producción (PRD).
En situaciones donde el servicio se inicie en un día que no coincida con el comienzo de un mes calendario, se aplicara el prorrateo. El prorrateo consistirá en calcular la proporción del servicio utilizado desde la fecha de inicio hasta el final del mes en curso y facturar únicamente por ese período inicial de manera proporcional.
El Contratista emitirá un informe a cada fin de mes indicando los incidentes y atenciones realizadas, así como las soluciones implementadas, además de recomendaciones de mejora de ser el caso.
El Banco revisará el informe como máximo en 5 días calendario y si hubiera alguna observación se le indicará al Contratista a través de correo electrónico al líder de proyecto del Contratista para la subsanación respectiva, para lo cual el Contratista tendrá 5 días calendarios adicionales como máximo para la subsanación. Una vez concluida la revisión por parte del Banco se emitirá un informe técnico y posteriormente el acta de conformidad para el pago.
Los responsables de la aprobación del informe técnico serán las áreas siguientes es:

- Subgerencia de Construcción
- Subgerencia de Producción
- Oficina de Seguridad Informática

El responsable del acta de conformidad será la Subgerencia de Innovación Digital de la Gerencia Banca Digital.

Los documentos a entregar por parte del Contratista para el pago serán:

- Carta simple dirigida al subgerente de compras de la gerencia de administración y logística
- Acta de conformidad suscrita por la Subgerencia de Innovación Digital de la Gerencia Banca Digital.
- Comprobante de pago.
- Informe técnico por parte de la Gerencia de TI especificado anteriormente.
- Copia del contrato.

La Entidad debe pagar las contraprestaciones pactadas a favor del Contratista dentro de los 15 días calendario siguiente a la conformidad de los servicios, siempre que se verifiquen las condiciones establecidas en el contrato.
Los informes remitidos en esta sección por parte del contratista serán coordinados para determinar el contenido de los mismos y el formato de estos

debiendo estar definidos en el plan de trabajo.

21.3. Componente Opcional

Cuenta DNI

El pago se efectuará contra el Acta de Conformidad del diseño, desarrollo e implementación del componente opcional Cuenta DNI. Este pago se realizará conforme al sistema de precio unitario. El precio unitario será determinado por la propuesta comercial presentada por el Contratista.

21.4. Servicio de Mejora Continua

El pago se llevará a cabo mensualmente, o según lo acordado con el Banco, una vez se haya recibido y aprobado el Acta de Conformidad correspondiente. Este pago se realizará conforme al sistema de precio unitario y basado en el consumo de horas utilizadas durante el periodo facturado. Los precios unitarios serán determinados por la propuesta comercial presentada por el Contratista.

22. GARANTÍA FINANCIERA

El postor adjudicado con la buena pro del concurso de méritos entregará para el perfeccionamiento del contrato la garantía financiera (carta fianza) de fiel cumplimiento de contrato.

La garantía que se presente debe ser incondicionales, solidarias, irrevocables y de realización automática en el país, al solo requerimiento del Banco de la Nación. Asimismo, debe ser emitida por empresas que se encuentren bajo la supervisión directa de la Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones y que cuenten con clasificación de riesgo B o superior. Asimismo, deben estar autorizadas para emitir garantías; o estar consideradas en la última lista de Bancos extranjeros de primera categoría que periódicamente publica el Banco Central de Reserva del Perú.

La garantía financiera (cartas fianza) deberá ser emitida a favor del Banco de la Nación, por los conceptos, montos y vigencias siguientes:

- Garantía de fiel cumplimiento del contrato: por una suma equivalente al diez por ciento (10%) del monto del contrato original, la misma que debe mantenerse vigente hasta la conformidad de la recepción de la prestación.

23. MEDIDAS DE SEGURIDAD

El CONTRASTISTA de la solución que debe considerar los Lineamientos para el Uso de Servicios de nube pública para entidades de la Administración Pública del Estado Peruano, para efectos de disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad, por lo cual queda obligado a cumplir y demostrar que, como mínimo, cumple con todas las medidas de seguridad de la NTP ISO/IEC 27001:2014 Tecnología de la Información, pertinentes para el nivel de disponibilidad requerido. Esto incluye instalaciones y personal. En su defecto podrá presentar la certificación global para nubes públicas ISO/IEC 27001:2013 de la nube ofertada. El CONTRASTISTA deberá ser un partner acreditado de la nube pública a ofertar. Las

medidas de seguridad podrán ser reemplazadas por otras siempre y cuando se acredite con las certificaciones respectivas que protegen igual o mejor el riesgo sobre los activos y se satisfacen los principios básicos en materia de seguridad de la información antes señalada.

24. MEDIDAS DE CONTROL DURANTE LA EJECUCIÓN CONTRATUAL Y CONFORMIDAD DEL SERVICIO

24.1. Administrador de Contrato

La Subgerencia de Innovación Digital de la Gerencia de Banca Digital, se encargará de la administración del contrato durante la ejecución del proyecto, siendo responsable de la supervisión y coordinación de la prestación contratada.

24.2. Área Responsable del Control de la Implementación

La Subgerencia de Producción, Subgerencia de Construcción de Aplicaciones y la Oficina de Seguridad de la Gerencia Tecnologías de Información serán responsables de la supervisión y coordinación del servicio de la implementación nueva plataforma bancaria para los canales digitales Banca Móvil y Banca por Internet.

25. CONFIDENCIALIDAD

- Toda la información entregada por el Banco de la Nación al postor del servicio tiene carácter confidencial.
- Cualquier copia, publicación, divulgación, distribución, total o parcial, interceptación sin autorización expresa por parte del Banco de la Nación o con fines no autorizados por el Banco de la Nación, de los documentos o información que describan la arquitectura y operación de las aplicaciones y base de datos del Banco de la Nación, serán motivo para la inmediata rescisión del vínculo contractual y del inicio de acciones legales que el Banco de la Nación considere. Su incumplimiento de la confidencialidad acarrea un incumplimiento a las obligaciones contractuales del presente termino de referencia.

26. RECURSOS DE PERSONAL DEL CONTRATISTA

A continuación, se detalla los perfiles profesionales mínimos requerido por perfil para la ejecución del proyecto de implementación, soporte técnico y del servicio de mejora continua de la nueva plataforma bancaria para los canales digitales Banca Móvil y Banca por Internet del Banco de la Nación:

26.1. Personal Clave del Proyecto

Personal para la ejecución del proyecto

UN (01) GERENTE DE PROYECTO	
Funciones	• Estará a cargo de la dirección general del proyecto, será el encargado de efectuar las coordinaciones directas con el Coordinador asignado por el BANCO durante la etapa de la implementación.

	• Informará sobre el avance de la implementación. • Elaborará las actas de reunión de trabajo. • Gestionará las pruebas de validación para el acta de conformidad • Coordinar con los implementadores el cumplimiento de los objetivos en el tiempo planificado. • Reportar los avances según el cronograma establecido en el plan de trabajo • Generar la documentación respectiva.

TRES (03) ESPECIALISTA DE NUBE	
Funciones	• Analizar los requisitos del cliente y traducirlos en una arquitectura de software adecuada. • Diseñar la estructura general del sistema, incluidos los componentes principales, las interfaces, los flujos de datos y la distribución física. • Evaluar y seleccionar las tecnologías y herramientas adecuadas para implementar la arquitectura propuesta. • Establecer patrones y estándares de diseño que guíen el desarrollo del software y promuevan la coherencia y la reutilización de código. • Definir principios arquitectónicos y prácticas recomendadas que mejoren la calidad y la mantenibilidad del software. • Identificar y gestionar requisitos no funcionales, como rendimiento, escalabilidad, seguridad, usabilidad y mantenibilidad. • Definir métricas y criterios de calidad para evaluar el cumplimiento de los requisitos no funcionales. • Configurar y desplegar servicios en la nube, como máquinas virtuales, contenedores, funciones sin servidor (serverless), bases de datos en la nube y servicios gestionados. • Automatizar el aprovisionamiento y la gestión de recursos en la nube utilizando herramientas de orquestación. • Analizar el uso de recursos en la nube y optimizar la configuración para minimizar los costos operativos, manteniendo al mismo tiempo el rendimiento y la disponibilidad del sistema. • Configurar herramientas de monitorización para supervisar el rendimiento y la disponibilidad de los servicios en la nube. • Analizar métricas y registros para identificar problemas de rendimiento y tomar medidas correctivas según sea necesario. • Implementar políticas de respaldo y recuperación de datos para proteger contra la pérdida de información y garantizar la continuidad del negocio en caso de fallos o desastres. • Realizar evaluaciones de seguridad y análisis de riesgos en el diseño y la implementación del sistema.

	• Identificar posibles vulnerabilidades y debilidades en la arquitectura y proponer soluciones para mitigar los riesgos. • Realizar pruebas de penetración y evaluaciones de seguridad para identificar posibles puntos de explotación. • Establecer políticas y estándares de seguridad para el desarrollo de software, incluidas las mejores prácticas de codificación segura. • Definir procedimientos y directrices para el manejo de datos sensibles, autenticación, autorización y gestión de accesos. • Implementar controles de acceso basados en roles y políticas de seguridad para proteger los recursos del sistema. • Automatizar el proceso de despliegue de aplicaciones en la nube utilizando herramientas propias del proveedor de nube seleccionado por el postor. • Configurar pipelines de CI/CD para integrar, probar y desplegar automáticamente cambios en el código a través de diferentes entornos (desarrollo, pruebas, producción). • Utilizar herramientas para definir y gestionar la infraestructura en la nube como código. • Automatizar la creación y configuración de recursos de infraestructura, como máquinas virtuales, redes y bases de datos, para mejorar la consistencia y la escalabilidad. • Implementar soluciones de monitoreo y observabilidad, para supervisar el rendimiento y la disponibilidad de las aplicaciones y la infraestructura en la nube. • Configurar alertas y notificaciones para detectar y responder rápidamente a problemas operativos o de rendimiento. • Gestionar la configuración de aplicaciones y servicios en la nube de forma centralizada y consistente utilizando herramientas de gestión de configuración. • Garantizar que las configuraciones sean versionadas y controladas adecuadamente para facilitar la reproducibilidad y la auditoría

26.2. Personal de Desarrollo y Soporte Técnico (Personal No Clave)

- **Personal de Desarrollo**

UN (01) PRODUCT DESIGNER	
Formación académica	Se requiere como mínimo Técnico en la especialidad de Diseño Gráfico, Diseño UX/UI y/o Afines.
Capacitación requerida	Curso de Capacitación en UX/UI y Figma o similares.
Experiencia	Experiencia mínima de cinco (05) años, el desarrollo de interfaces para aplicaciones web y móviles en el sector financiero, público o privado.

Funciones	• Definir y guiar el proceso de diseño completo utilizando las metodologías establecidas desde la identificación de insights hasta la conceptualización, validación, prototipado, interacción, diseño visual, lanzamiento y optimizaciones de la solución. • Ser partícipe de los procesos de ideación del equipo y generar la mayor cantidad de ideas posibles. • Fomentar el mantenimiento y creación de herramientas y documentación de diseño como Design Systems, micro interacciones y repositorios de investigaciones. • Fomentar la co-creación con clientes, usuarios y stakeholders, en la etapa de diseño. • Participar en todas las etapas de un proyecto, no únicamente en las relacionadas a la especialidad del rol.

DOS (02) DESARROLLADOR DE APLICACIONES MÓVILES	
Formación académica	Se requiere como mínimo egresado universitario o Técnico en Ingeniería de Sistemas y/o Ingeniería de Cómputo y/o Ingeniería Informática y/o Ingeniería de Telecomunicaciones y/o Ingeniería Industrial y/o Ingeniería Electrónica o afines.
Capacitación requerida	Certificación o curso en el desarrollo de aplicaciones plataformas Móvil
Experiencia	Experiencia mínima de cinco (05) años en el desarrollo de aplicaciones móviles utilizando tecnologías nativas o afines en el sector financiero o afines, público o privado.
Funciones	● Desarrollar la interfaz de usuario de aplicaciones móviles en diversos sectores. ● Utilizar herramientas de desarrollo y APIs proporcionadas para acceder a servicios específicos, como consultas de datos, transferencias de información, pagos, pasarelas de pago, servicios de autenticación y sistemas de gestión de cuentas, entre otros. ● Integrar APIs de servicios externos, como servicios de autenticación, funcionales del Core Bancario, servicios de geolocalización o servicios de pago, entre otros. ● Integrar la interfaz de usuario con sistemas y servicios, como APIs específicas del sector, pasarelas de pago, servicios de autenticación y sistemas de gestión de datos. ● Implementar medidas de seguridad robustas para proteger la información confidencial de los usuarios, como datos personales y detalles de transacciones. ● Realizar coordinaciones con el personal relevante para asegurar la implementación exitosa de la solución. ● Ser responsable de la implementación, instalación y configuración de las soluciones desarrolladas. ● Utilizar frameworks y bibliotecas modernas para desarrollar componentes de interfaz de usuario interactivos y dinámicos. ● Optimizar el rendimiento de las aplicaciones móviles mediante

	técnicas como la carga diferida de módulos y la optimización del tamaño del paquete. ● Realizar pruebas de integración para validar la interacción entre los componentes de la aplicación y garantizar su funcionalidad en conjunto. ● Elaborar la documentación de la solución implementada. ● Utilizar herramientas para agilizar la creación y despliegue de aplicaciones cuando sea adecuado.

DOS (02) CERTIFICADOR DE QA	
Formación académica	Se requiere como mínimo egresado universitario o técnico en Ingeniería de Sistemas y/o Ingeniería de Cómputo y/o Ingeniería Informática y/o Ingeniería de Telecomunicaciones y/o Ingeniería Industrial y/o Ingeniería Electrónica o afines.
Capacitación requerida	Certificación o curso completado en ISTQB Foundation
Experiencia	Experiencia mínima de cinco (05) años realizando actividades de pruebas automatizadas en el sector financiero, público o privado.
Funciones	• Desarrollar criterios y estándares de calidad para el desarrollo de software, teniendo en cuenta las necesidades del cliente, las regulaciones aplicables y las mejores prácticas de la industria. • Revisar y analizar los requisitos del cliente para garantizar que sean claros, completos y alcanzables desde una perspectiva de calidad. • Diseñar planes de prueba detallados que abarquen todos los aspectos funcionales y no funcionales del software, así como pruebas de performance y stress, incluida la funcionalidad, la usabilidad, el rendimiento y la seguridad. • Realizar pruebas exhaustivas del software según el plan establecido, utilizando técnicas como pruebas de unidad, pruebas de integración, pruebas de aceptación del usuario, pruebas de carga, etc. • Analizar los resultados de las pruebas para identificar defectos, anomalías y áreas de mejora en el software. • Preparar informes detallados sobre los resultados de las pruebas, destacando los problemas encontrados y proporcionando recomendaciones para su resolución. • Registrar y rastrear los defectos identificados durante las pruebas, asegurándose de que se aborden de manera oportuna y adecuada. • Diseñar, desarrollar y mantener casos de prueba automatizados utilizando herramientas y frameworks de automatización de pruebas. • Escribir scripts de prueba que cubran diferentes aspectos del software, incluyendo funcionalidades clave, flujos de trabajo críticos y escenarios de uso comunes. • Integrar los casos de prueba automatizados en pipelines de CI/CD para ejecutar pruebas de forma automática en cada nueva versión del

	software. • Ejecutar pruebas automatizadas de forma regular y sistemática para identificar defectos, anomalías y problemas de rendimiento en el software. • Analizar los resultados de las pruebas automatizadas para identificar patrones, tendencias y áreas de mejora en la calidad del software.

UN (01) DESARROLLADOR WEB	
Formación académica	Se requiere como mínimo egresado universitario o técnico en Ingeniería de Sistemas y/o Ingeniería de Cómputo y/o Ingeniería Informática y/o Ingeniería de Telecomunicaciones y/o Ingeniería Industrial y/o Ingeniería Electrónica o afines.
Capacitación requerida	Certificación o cursos en el desarrollo de aplicaciones plataformas WEB
Experiencia	Experiencia mínima de cinco (05) años en el desarrollo de aplicaciones web utilizando diversas tecnologías en el sector financiero, público o privado.
Funciones	● Desarrollar la interfaz de usuario de aplicaciones web. ● Utilizar herramientas de desarrollo y APIs, RESTful o GraphQL proporcionadas para acceder a servicios específicos, como consultas de datos, transferencias de información, pagos, entre otros. ● Integrar la interfaz de usuario con sistemas y servicios, como APIs, RESTful o GraphQL específicas del sector, pasarelas de pago, servicios de autenticación y sistemas de gestión de datos. ● Integrar APIs de servicios externos, como servicios de autenticación, funcionales del Core Bancario, servicios de geolocalización o servicios de pago, entre otros. ● Implementar medidas de seguridad robustas para proteger la información confidencial de los usuarios, como datos personales y detalles de transacciones. ● Realizar coordinaciones con el personal relevante para asegurar la implementación exitosa de la solución. ● Ser responsable de la implementación, instalación y configuración de las soluciones desarrolladas. ● Utilizar frameworks y bibliotecas modernas para desarrollar componentes de interfaz de usuario interactivos y dinámicos. ● Optimizar el rendimiento de las aplicaciones web mediante técnicas como la carga diferida de módulos y la optimización del tamaño del paquete. ● Realizar pruebas de integración para validar la interacción entre los componentes de la aplicación y garantizar su funcionalidad en conjunto. ● Realizar pruebas de rendimiento y análisis de rendimiento para identificar y solucionar cuellos de botella de rendimiento.

	● Elaborar la documentación de la solución implementada. ● Utilizar herramientas para agilizar la creación y despliegue de aplicaciones cuando sea adecuado.

UNO (01) DESARROLLADOR FULL STACK	
Formación académica	Se requiere como mínimo egresado universitario o técnico en Ingeniería de Sistemas y/o Ingeniería de Cómputo y/o Ingeniería Informática y/o Ingeniería de Telecomunicaciones y/o Ingeniería Industrial y/o Ingeniería Electrónica o afines.
Capacitación requerida	Certificado o cursos en el desarrollo de APIS
Experiencia	Experiencia mínima de cinco (05) años realizando actividades de desarrollo de API Rest con tecnologías Java SpringBoot y/o afines en el sector financiero, público o privado.
Funciones	● Desarrollar tanto el frontend como el backend de aplicaciones web y móviles. ● Implementar interfaces de usuario utilizando herramientas y componentes modernos para crear experiencias interactivas y dinámicas. ● Desarrollar y mantener APIs para la comunicación entre el cliente y el servidor. ● Optimizar el rendimiento de las aplicaciones mediante diversas técnicas, como la carga diferida de módulos, la optimización del tamaño del paquete y la implementación de técnicas de almacenamiento en caché. ● Realizar pruebas y análisis de rendimiento para identificar y solucionar cuellos de botella. ● Integrar servicios externos, como servicios de autenticación, sistemas centrales, servicios de geolocalización o servicios de pago, en las aplicaciones. ● Implementar medidas de seguridad robustas para proteger la información confidencial de los usuarios, como datos personales y detalles de transacciones. ● Utilizar herramientas de desarrollo para agilizar la creación y despliegue de aplicaciones cuando sea adecuado. ● Realizar coordinaciones con el personal relevante para asegurar la implementación exitosa de la solución.

	● Ser responsable de la implementación, instalación y configuración de las soluciones desarrolladas. ● Diseñar y desarrollar APIs para proporcionar acceso a los recursos y servicios de la aplicación desde el frontend y otras aplicaciones. ● Implementar endpoints API para realizar operaciones CRUD (Crear, Leer, Actualizar, Borrar) en la base de datos y manipular datos de manera eficiente. ● Utilizar herramientas y frameworks para mapear objetos a tablas de base de datos y realizar operaciones de consulta y manipulación de datos. ● Diseñar y optimizar modelos de datos y esquemas de bases de datos relacionales o NoSQL para satisfacer los requisitos de la aplicación. ● Realizar pruebas de integración para validar la interacción entre los componentes de la aplicación y garantizar su funcionalidad en conjunto. ● Elaborar la documentación de la solución implementada.

UN (01) DESARROLLADOR COBOL	
Formación académica	Curso de Especialización en el desarrollo de aplicaciones con Cobol
Capacitación requerida	Certificación en el desarrollo de aplicaciones en Cobol
Experiencia	Experiencia mínima de cinco (05) años realizando actividades de desarrollo en Cobol relacionado a Mainframe en el sector financiero, público o privado.
Funciones	• Desarrollo de soluciones COBOL para la organización. • Creación de aplicaciones in house utilizando COBOL. • Depuración y mantenimiento de código COBOL existente. • Definición y organización de proyectos de forma continua. • Reportar y resolver problemas relacionados a proyectos COBOL. • Identificar y manejar riesgos y problemas técnicos. • Informar sobre el estado y desarrollo del proyecto a los miembros senior del equipo. • Participar en las reuniones del proyecto con la gerencia y otros miembros del equipo

- **Perfiles de Soporte Técnico (Personal No Clave)**

UN (01) DESARROLLADOR DE APLICACIONES MÓVILES SOPORTE TÉCNICO	
Formación académica	Se requiere como mínimo egresado universitario o técnico en Ingeniería de Sistemas y/o Ingeniería de Cómputo y/o Ingeniería Informática y/o Ingeniería de Telecomunicaciones y/o Ingeniería Industrial y/o Ingeniería Electrónica o afines.

Capacitación requerida	Certificación o curso en el desarrollo de aplicaciones plataformas Móvil
Experiencia	Experiencia mínima de cinco (05) años en el desarrollo de aplicaciones móviles utilizando tecnologías nativas o afines en el sector financiero, público o privado.
Funciones	● Desarrollar la interfaz de usuario de aplicaciones móviles en diversos sectores. ● Utilizar herramientas de desarrollo y APIs proporcionadas para acceder a servicios específicos, como consultas de datos, transferencias de información, pagos, pasarelas de pago, servicios de autenticación y sistemas de gestión de cuentas, entre otros. ● Integrar APIs de servicios externos, como servicios de autenticación, funcionales del Core Bancario, servicios de geolocalización o servicios de pago, entre otros. ● Integrar la interfaz de usuario con sistemas y servicios, como APIs específicas del sector, pasarelas de pago, servicios de autenticación y sistemas de gestión de datos. ● Implementar medidas de seguridad robustas para proteger la información confidencial de los usuarios, como datos personales y detalles de transacciones. ● Realizar coordinaciones con el personal relevante para asegurar la implementación exitosa de la solución. ● Ser responsable de la implementación, instalación y configuración de las soluciones desarrolladas. ● Utilizar frameworks y bibliotecas modernas para desarrollar componentes de interfaz de usuario interactivos y dinámicos. ● Optimizar el rendimiento de las aplicaciones móviles mediante técnicas como la carga diferida de módulos y la optimización del tamaño del paquete. ● Realizar pruebas de integración para validar la interacción entre los componentes de la aplicación y garantizar su funcionalidad en conjunto. ● Elaborar la documentación de la solución implementada. ● Utilizar herramientas para agilizar la creación y despliegue de aplicaciones cuando sea adecuado.

UN (01) DESARROLLADOR WEB SOPORTE TÉCNICO	
Formación académica	Se requiere como mínimo egresado universitario o técnico en Ingeniería de Sistemas y/o Ingeniería de Cómputo y/o Ingeniería Informática y/o Ingeniería de Telecomunicaciones y/o Ingeniería Industrial y/o Ingeniería Electrónica o afines.
Capacitación requerida	Certificación o cursos en el desarrollo de aplicaciones plataformas WEB

Experiencia	Experiencia mínima de cinco (05) años en el desarrollo de aplicaciones web utilizando diversas tecnologías en el sector financiero, público o privado.
Funciones	● Desarrollar la interfaz de usuario de aplicaciones web. ● Utilizar herramientas de desarrollo y APIs, RESTful o GraphQL proporcionadas para acceder a servicios específicos, como consultas de datos, transferencias de información, pagos, entre otros. ● Integrar la interfaz de usuario con sistemas y servicios, como APIs, RESTful o GraphQL específicas del sector, pasarelas de pago, servicios de autenticación y sistemas de gestión de datos. ● Integrar APIs de servicios externos, como servicios de autenticación, funcionales del Core Bancario, servicios de geolocalización o servicios de pago, entre otros. ● Implementar medidas de seguridad robustas para proteger la información confidencial de los usuarios, como datos personales y detalles de transacciones. ● Realizar coordinaciones con el personal relevante para asegurar la implementación exitosa de la solución. ● Ser responsable de la implementación, instalación y configuración de las soluciones desarrolladas. ● Utilizar frameworks y bibliotecas modernas para desarrollar componentes de interfaz de usuario interactivos y dinámicos. ● Optimizar el rendimiento de las aplicaciones web mediante técnicas como la carga diferida de módulos y la optimización del tamaño del paquete. ● Realizar pruebas de integración para validar la interacción entre los componentes de la aplicación y garantizar su funcionalidad en conjunto. ● Realizar pruebas de rendimiento y análisis de rendimiento para identificar y solucionar cuellos de botella de rendimiento. ● Elaborar la documentación de la solución implementada. ● Utilizar herramientas para agilizar la creación y despliegue de aplicaciones cuando sea adecuado.

UN (01) CERTIFICADOR QA SOPORTE TÉCNICO	
Formación académica	Se requiere como mínimo egresado universitario o técnico en Ingeniería de Sistemas y/o Ingeniería de Cómputo y/o Ingeniería Informática y/o Ingeniería de Telecomunicaciones y/o Ingeniería Industrial y/o Ingeniería Electrónica o afines.
Capacitación requerida	Certificación en ISTQB Foundation
Experiencia	Experiencia mínima de cinco (05) años realizando actividades de pruebas automatizadas en el sector público o privado.

Funciones	• Desarrollar criterios y estándares de calidad para el desarrollo de software, teniendo en cuenta las necesidades del cliente, las regulaciones aplicables y las mejores prácticas de la industria. • Revisar y analizar los requisitos del cliente para garantizar que sean claros, completos y alcanzables desde una perspectiva de calidad. • Diseñar planes de prueba detallados que abarquen todos los aspectos funcionales y no funcionales del software, así como pruebas de performance y stress, incluida la funcionalidad, la usabilidad, el rendimiento y la seguridad. • Realizar pruebas exhaustivas del software según el plan establecido, utilizando técnicas como pruebas de unidad, pruebas de integración, pruebas de aceptación del usuario, pruebas de carga, etc. • Analizar los resultados de las pruebas para identificar defectos, anomalías y áreas de mejora en el software. • Preparar informes detallados sobre los resultados de las pruebas, destacando los problemas encontrados y proporcionando recomendaciones para su resolución. • Registrar y rastrear los defectos identificados durante las pruebas, asegurándose de que se aborden de manera oportuna y adecuada. • Diseñar, desarrollar y mantener casos de prueba automatizados utilizando herramientas y frameworks de automatización de pruebas. • Escribir scripts de prueba que cubran diferentes aspectos del software, incluyendo funcionalidades clave, flujos de trabajo críticos y escenarios de uso comunes. • Integrar los casos de prueba automatizados en pipelines de CI/CD para ejecutar pruebas de forma automática en cada nueva versión del software. • Ejecutar pruebas automatizadas de forma regular y sistemática para identificar defectos, anomalías y problemas de rendimiento en el software. • Analizar los resultados de las pruebas automatizadas para identificar patrones, tendencias y áreas de mejora en la calidad del software.

UN (01) DESARROLLADOR FULL STACK SOPORTE TÉCNICO	
Formación académica	Se requiere como mínimo egresado universitario o técnico en Ingeniería de Sistemas y/o Ingeniería de Cómputo y/o Ingeniería Informática y/o Ingeniería de Telecomunicaciones y/o Ingeniería Industrial y/o Ingeniería Electrónica o afines.
Capacitación requerida	Certificado o curso en el desarrollo de APIS o desarrollo de software acordes al requerimiento
Experiencia	Experiencia mínima de cinco (05) años realizando actividades de desarrollo de API Rest con tecnologías Java springboot y/o afines en el sector público o privado.
Funciones	● Desarrollar tanto el frontend como el backend de aplicaciones

	web y móviles. ● Implementar interfaces de usuario utilizando herramientas y componentes modernos para crear experiencias interactivas y dinámicas. ● Desarrollar y mantener APIs para la comunicación entre el cliente y el servidor. ● Optimizar el rendimiento de las aplicaciones mediante diversas técnicas, como la carga diferida de módulos, la optimización del tamaño del paquete y la implementación de técnicas de almacenamiento en caché. ● Realizar pruebas y análisis de rendimiento para identificar y solucionar cuellos de botella. ● Integrar servicios externos, como servicios de autenticación, sistemas centrales, servicios de geolocalización o servicios de pago, en las aplicaciones. ● Implementar medidas de seguridad robustas para proteger la información confidencial de los usuarios, como datos personales y detalles de transacciones. ● Utilizar herramientas de desarrollo para agilizar la creación y despliegue de aplicaciones cuando sea adecuado. ● Realizar coordinaciones con el personal relevante para asegurar la implementación exitosa de la solución. ● Ser responsable de la implementación, instalación y configuración de las soluciones desarrolladas. ● Diseñar y desarrollar APIs para proporcionar acceso a los recursos y servicios de la aplicación desde el frontend y otras aplicaciones. ● Implementar endpoints API para realizar operaciones CRUD (Crear, Leer, Actualizar, Borrar) en la base de datos y manipular datos de manera eficiente. ● Utilizar herramientas y frameworks para mapear objetos a tablas de base de datos y realizar operaciones de consulta y manipulación de datos. ● Diseñar y optimizar modelos de datos y esquemas de bases de datos relacionales o NoSQL para satisfacer los requisitos de la aplicación. ● Realizar pruebas de integración para validar la interacción entre los componentes de la aplicación y garantizar su funcionalidad en conjunto. ● Elaborar la documentación de la solución implementada.

UN (01) ESPECIALISTA DE NUBE SOPORTE TÉCNICO	
Formación académica	Se requiere como mínimo egresado universitario o técnico en Ingeniería de Sistemas y/o Ingeniería de Cómputo y/o Ingeniería Informática y/o Ingeniería de Telecomunicaciones y/o Ingeniería Industrial y/o Ingeniería Electrónica o afines.

Capacitación requerida	Certificado o curso en arquitectura y/o seguridad asociado de la marca de la Nube a ofertar.
Experiencia	Deberá acreditar experiencia mínima de 2 años en implementación y/o despliegue en soluciones de seguridad cloud.
Funciones	• Analizar los requisitos del cliente y traducirlos en una arquitectura de software adecuada. • Diseñar la estructura general del sistema, incluidos los componentes principales, las interfaces, los flujos de datos y la distribución física. • Evaluar y seleccionar las tecnologías y herramientas adecuadas para implementar la arquitectura propuesta. • Establecer patrones y estándares de diseño que guíen el desarrollo del software y promuevan la coherencia y la reutilización de código. • Definir principios arquitectónicos y prácticas recomendadas que mejoren la calidad y la mantenibilidad del software. • Identificar y gestionar requisitos no funcionales, como rendimiento, escalabilidad, seguridad, usabilidad y mantenibilidad. • Definir métricas y criterios de calidad para evaluar el cumplimiento de los requisitos no funcionales. • Configurar y desplegar servicios en la nube, como máquinas virtuales, contenedores, funciones sin servidor (serverless), bases de datos en la nube y servicios gestionados. • Automatizar el aprovisionamiento y la gestión de recursos en la nube utilizando herramientas de orquestación. • Analizar el uso de recursos en la nube y optimizar la configuración para minimizar los costos operativos, manteniendo al mismo tiempo el rendimiento y la disponibilidad del sistema. • Configurar herramientas de monitorización para supervisar el rendimiento y la disponibilidad de los servicios en la nube. • Analizar métricas y registros para identificar problemas de rendimiento y tomar medidas correctivas según sea necesario. • Implementar políticas de respaldo y recuperación de datos para proteger contra la pérdida de información y garantizar la continuidad del negocio en caso de fallos o desastres. • Realizar evaluaciones de seguridad y análisis de riesgos en el diseño y la implementación del sistema. • Identificar posibles vulnerabilidades y debilidades en la arquitectura y proponer soluciones para mitigar los riesgos. • Realizar pruebas de penetración y evaluaciones de seguridad para identificar posibles puntos de explotación. • Establecer políticas y estándares de seguridad para el desarrollo de software, incluidas las mejores prácticas de codificación segura. • Definir procedimientos y directrices para el manejo de datos

	sensibles, autenticación, autorización y gestión de accesos. • Implementar controles de acceso basados en roles y políticas de seguridad para proteger los recursos del sistema. • Automatizar el proceso de despliegue de aplicaciones en la nube utilizando herramientas propias del proveedor de nube seleccionado por el postor. • Configurar pipelines de CI/CD para integrar, probar y desplegar automáticamente cambios en el código a través de diferentes entornos (desarrollo, pruebas, producción). • Utilizar herramientas para definir y gestionar la infraestructura en la nube como código. • Automatizar la creación y configuración de recursos de infraestructura, como máquinas virtuales, redes y bases de datos, para mejorar la consistencia y la escalabilidad. • Implementar soluciones de monitoreo y observabilidad, para supervisar el rendimiento y la disponibilidad de las aplicaciones y la infraestructura en la nube. • Configurar alertas y notificaciones para detectar y responder rápidamente a problemas operativos o de rendimiento. • Gestionar la configuración de aplicaciones y servicios en la nube de forma centralizada y consistente utilizando herramientas de gestión de configuración. • Garantizar que las configuraciones sean versionadas y controladas adecuadamente para facilitar la reproducibilidad y la auditoría

26.3. Recursos de Personal para el Servicio de Mejora Continua (Personal No Clave)

Para la etapa de mejora continua, que iniciará una vez terminado el desarrollo del proyecto, se requerirá los siguientes perfiles profesionales:

UN (01) TECHNICAL LEAD MEJORA CONTINUA	
Formación académica	Profesional Titulado, Bachiller, Profesional Técnico, Técnico, egresado universitario o técnico en Ingeniería de Sistemas y/o Ingeniería de Cómputo y/o Ingeniería Informática y/o Ingeniería de Telecomunicaciones y/o Ingeniería Industrial y/o Ingeniería Electrónica o afines.
Capacitación requerida	Certificaciones o cursos técnicos en lenguajes de programación Web y Mobile.
Experiencia	Experiencia mínima de un (04) liderando equipos de trabajo en desarrollo de productos tecnológicos y/o afines en el sector público o privado.
Funciones	• Diseñar la arquitectura técnica de las soluciones de software, asegurando que cumplan con los requisitos funcionales y no funcionales del Banco, así como con las mejores prácticas de la industria. • Seleccionar tecnologías y plataformas apropiadas que se alineen con

	la estrategia tecnológica del Banco y promuevan la escalabilidad, la seguridad y el rendimiento. • Liderar y supervisar equipos de desarrollo, incluidos ingenieros de software, arquitectos de software y especialistas en QA, proporcionando orientación técnica, resolución de problemas y apoyo en la toma de decisiones. • Coordinar con los equipos de desarrollo y gestión de proyectos para planificar y estimar los esfuerzos de desarrollo de software, identificando dependencias, riesgos y recursos necesarios. • Definir cronogramas realistas y establecer hitos claros para el desarrollo e implementación de las soluciones de software. • Realizar gestión de cambio de procesos (con Bizagi). • Coordinar con usuarios internos respecto a cambios en el proceso. • Coordinar con concesionarios respecto a cambios en el proceso. • Realizar pruebas de integración internas y documentación. • Relevamiento de Procesos (Esquema AS-IS/To-Be). • Seguimiento de Actividades (Cronogramas, Actividades, Costos) - Herramientas CRM.

UN (01) DESARROLLADOR DE APLICACIONES MÓVILES MEJORA CONTINUA	
Formación académica	Se requiere como mínimo egresado universitario o técnico en Ingeniería de Sistemas y/o Ingeniería de Cómputo y/o Ingeniería Informática y/o Ingeniería de Telecomunicaciones y/o Ingeniería Industrial y/o Ingeniería Electrónica o afines.
Capacitación requerida	Certificación o curso en el desarrollo de aplicaciones plataformas Móvil
Experiencia	Experiencia mínima de cinco (05) años en el desarrollo de aplicaciones móviles utilizando tecnologías nativas o afines en el sector financiero, público o privado.
Funciones	● Desarrollar la interfaz de usuario de aplicaciones móviles en diversos sectores. ● Utilizar herramientas de desarrollo y APIs proporcionadas para acceder a servicios específicos, como consultas de datos, transferencias de información, pagos, pasarelas de pago, servicios de autenticación y sistemas de gestión de cuentas, entre otros. ● Integrar APIs de servicios externos, como servicios de autenticación, funcionales del Core Bancario, servicios de geolocalización o servicios de pago, entre otros. ● Integrar la interfaz de usuario con sistemas y servicios, como APIs específicas del sector, pasarelas de pago, servicios de autenticación y sistemas de gestión de datos. ● Implementar medidas de seguridad robustas para proteger la información confidencial de los usuarios, como datos personales y detalles de transacciones.

	● Realizar coordinaciones con el personal relevante para asegurar la implementación exitosa de la solución. ● Ser responsable de la implementación, instalación y configuración de las soluciones desarrolladas. ● Utilizar frameworks y bibliotecas modernas para desarrollar componentes de interfaz de usuario interactivos y dinámicos. ● Optimizar el rendimiento de las aplicaciones móviles mediante técnicas como la carga diferida de módulos y la optimización del tamaño del paquete. ● Realizar pruebas de integración para validar la interacción entre los componentes de la aplicación y garantizar su funcionalidad en conjunto. ● Elaborar la documentación de la solución implementada. ● Utilizar herramientas para agilizar la creación y despliegue de aplicaciones cuando sea adecuado.

UN (01) DESARROLLADOR WEB MEJORA CONTINUA	
Formación académica	Se requiere como mínimo egresado universitario o técnico en Ingeniería de Sistemas y/o Ingeniería de Cómputo y/o Ingeniería Informática y/o Ingeniería de Telecomunicaciones y/o Ingeniería Industrial y/o Ingeniería Electrónica o afines.
Capacitación requerida	Certificación o cursos en el desarrollo de aplicaciones plataformas WEB
Experiencia	Experiencia mínima de cinco (05) años en el desarrollo de aplicaciones web utilizando diversas tecnologías en el sector financiero, público o privado.
Funciones	● Desarrollar la interfaz de usuario de aplicaciones web. ● Utilizar herramientas de desarrollo y APIs, RESTful o GraphQL proporcionadas para acceder a servicios específicos, como consultas de datos, transferencias de información, pagos, entre otros. ● Integrar la interfaz de usuario con sistemas y servicios, como APIs, RESTful o GraphQL específicas del sector, pasarelas de pago, servicios de autenticación y sistemas de gestión de datos. ● Integrar APIs de servicios externos, como servicios de autenticación, funcionales del Core Bancario, servicios de geolocalización o servicios de pago, entre otros. ● Implementar medidas de seguridad robustas para proteger la información confidencial de los usuarios, como datos personales y detalles de transacciones. ● Realizar coordinaciones con el personal relevante para asegurar la implementación exitosa de la solución. ● Ser responsable de la implementación, instalación y configuración de las soluciones desarrolladas. ● Utilizar frameworks y bibliotecas modernas para desarrollar

	componentes de interfaz de usuario interactivos y dinámicos. ● Optimizar el rendimiento de las aplicaciones web mediante técnicas como la carga diferida de módulos y la optimización del tamaño del paquete. ● Realizar pruebas de integración para validar la interacción entre los componentes de la aplicación y garantizar su funcionalidad en conjunto. ● Realizar pruebas de rendimiento y análisis de rendimiento para identificar y solucionar cuellos de botella de rendimiento. ● Elaborar la documentación de la solución implementada. ● Utilizar herramientas para agilizar la creación y despliegue de aplicaciones cuando sea adecuado.

UN (01) DESARROLLADOR FULL STACK MEJORA CONTINUA	
Formación académica	Se requiere como mínimo egresado universitario o técnico en Ingeniería de Sistemas y/o Ingeniería de Cómputo y/o Ingeniería Informática y/o Ingeniería de Telecomunicaciones y/o Ingeniería Industrial y/o Ingeniería Electrónica o afines.
Capacitación requerida	Certificado o curso en el desarrollo de APIS o desarrollo de software acordes al requerimiento
Experiencia	Experiencia mínima de cinco (05) años realizando actividades de desarrollo de API Rest con tecnologías Java springboot y/o afines en el sector público o privado.
Funciones	● Desarrollar tanto el frontend como el backend de aplicaciones web y móviles. ● Implementar interfaces de usuario utilizando herramientas y componentes modernos para crear experiencias interactivas y dinámicas. ● Desarrollar y mantener APIs para la comunicación entre el cliente y el servidor. ● Optimizar el rendimiento de las aplicaciones mediante diversas técnicas, como la carga diferida de módulos, la optimización del tamaño del paquete y la implementación de técnicas de almacenamiento en caché. ● Realizar pruebas y análisis de rendimiento para identificar y solucionar cuellos de botella. ● Integrar servicios externos, como servicios de autenticación, sistemas centrales, servicios de geolocalización o servicios de pago, en las aplicaciones. ● Implementar medidas de seguridad robustas para proteger la información confidencial de los usuarios, como datos personales y detalles de transacciones. ● Utilizar herramientas de desarrollo para agilizar la creación y despliegue de aplicaciones cuando sea adecuado. ● Realizar coordinaciones con el personal relevante para asegurar la implementación exitosa de la solución.

	● Ser responsable de la implementación, instalación y configuración de las soluciones desarrolladas. ● Diseñar y desarrollar APIs para proporcionar acceso a los recursos y servicios de la aplicación desde el frontend y otras aplicaciones. ● Implementar endpoints API para realizar operaciones CRUD (Crear, Leer, Actualizar, Borrar) en la base de datos y manipular datos de manera eficiente. ● Utilizar herramientas y frameworks para mapear objetos a tablas de base de datos y realizar operaciones de consulta y manipulación de datos. ● Diseñar y optimizar modelos de datos y esquemas de bases de datos relacionales o NoSQL para satisfacer los requisitos de la aplicación. ● Realizar pruebas de integración para validar la interacción entre los componentes de la aplicación y garantizar su funcionalidad en conjunto. ● Elaborar la documentación de la solución implementada.

UN (01) CERTIFICADOR QA MEJORA CONTINUA	
Formación académica	Se requiere como mínimo egresado universitario o técnico en Ingeniería de Sistemas y/o Ingeniería de Cómputo y/o Ingeniería Informática y/o Ingeniería de Telecomunicaciones y/o Ingeniería Industrial y/o Ingeniería Electrónica o afines.
Capacitación requerida	Certificación o curso completado en ISTQB Foundation
Experiencia	Experiencia mínima de cinco (05) años realizando actividades de pruebas automatizadas en el sector financiero, público o privado.
Funciones	• Desarrollar criterios y estándares de calidad para el desarrollo de software, teniendo en cuenta las necesidades del cliente, las regulaciones aplicables y las mejores prácticas de la industria. • Revisar y analizar los requisitos del cliente para garantizar que sean claros, completos y alcanzables desde una perspectiva de calidad. • Diseñar planes de prueba detallados que abarquen todos los aspectos funcionales y no funcionales del software, así como pruebas de performance y stress, incluida la funcionalidad, la usabilidad, el rendimiento y la seguridad. • Realizar pruebas exhaustivas del software según el plan establecido, utilizando técnicas como pruebas de unidad, pruebas de integración, pruebas de aceptación del usuario, pruebas de carga, etc. • Analizar los resultados de las pruebas para identificar defectos, anomalías y áreas de mejora en el software. • Preparar informes detallados sobre los resultados de las pruebas, destacando los problemas encontrados y proporcionando recomendaciones para su resolución. • Registrar y rastrear los defectos identificados durante las pruebas,

	asegurándose de que se aborden de manera oportuna y adecuada. • Diseñar, desarrollar y mantener casos de prueba automatizados utilizando herramientas y frameworks de automatización de pruebas. • Escribir scripts de prueba que cubran diferentes aspectos del software, incluyendo funcionalidades clave, flujos de trabajo críticos y escenarios de uso comunes. • Integrar los casos de prueba automatizados en pipelines de CI/CD para ejecutar pruebas de forma automática en cada nueva versión del software. • Ejecutar pruebas automatizadas de forma regular y sistemática para identificar defectos, anomalías y problemas de rendimiento en el software. • Analizar los resultados de las pruebas automatizadas para identificar patrones, tendencias y áreas de mejora en la calidad del software.

26.4. Consideraciones sobre el personal del contratista

El proveedor ganador de la buena pro deberá asegurar que el equipo asignado al proyecto cuente con las habilidades, experiencia y disponibilidad requeridas para llevar a cabo las actividades establecidas en el plan de trabajo, cumpliendo con los plazos y entregables acordados. Cualquier ajuste en la composición del equipo deberá ser comunicado y aprobado previamente por el Banco de la Nación, siempre y cuando no afecte el costo total del servicio ni genere pagos adicionales.

El proveedor ganador de la buena pro será el único responsable de incorporar y gestionar el personal necesario a fin de garantizar el cumplimiento del plan de trabajo establecido, sin que esto implique modificaciones en el costo total del servicio ni pagos adicionales o diferenciados por parte del Banco de la Nación.

El proveedor adjudicado con la buena pro deberá garantizar que cada miembro del equipo tenga una asignación clara y definida de responsabilidades, evitando la sobrecarga de trabajo y asegurando la calidad y eficiencia en la ejecución de las tareas.

El proveedor ganador con la buena pro deberá asegurar que el personal profesional asignado al proyecto se dedique exclusivamente a las tareas establecidas en el plan de trabajo, sin realizar actividades en paralelo que puedan afectar el cumplimiento de los plazos y entregables acordados.

De producirse un reemplazo de algún personal por motivo de fuerza mayor, el Contratista comunicará la salida del personal con un plazo máximo de 24 horas de ocurrido el evento y deberá realizar el reemplazo, en un plazo máximo de cinco (5) días calendario, en caso contrario será aplicable las penalidades correspondientes (ver 35.2. Otras Penalidades). Se indica que el personal reemplazante debe tener igual o superior perfil que el reemplazado y deberá contar con la aprobación del Bando de la Nación.

La Formación Académica, capacitación y experiencia exigida para el personal no clave requeridos en el numerales 26.3 Personal de Desarrollo y Soporte Técnico y 26.2 Recursos de personal para la Mejora Continua del Servicio, deberán ser

acreditado por el postor adjudicado con la Buena Pro, a la suscripción del contrato con la presentación de la documentación que acredite las condiciones establecidas. Todos los cursos de especialización técnica deberán tener un mínimo de 12 horas de duración como mínimo.

El Banco de la Nación podrá solicitar al Contratista el reemplazo de miembros de su personal, comprometiéndose el Contratista a asignar personal de calificaciones similares o superiores al(los) miembro(s) a ser reemplazado(s). De aplicarse este caso, el Contratista debe reemplazar al personal en un plazo máximo de tres (3) días calendario, después de la aprobación realizada por el Banco de la Nación a través de correo electrónico.

27. SUBCONTRATACIÓN

El Proveedor es el único responsable ante el Banco de cumplir con las condiciones técnicas y prestaciones establecidas en los presentes términos de referencia, pudiendo subcontratar actividades complementarias hasta por el 40% del monto del contrato inicial, a excepción del objeto principal de contrato que es implementar los canales digitales Banca Móvil y Banca por Internet del Banco de la Nación.

28. RESPONSABILIDAD DEL PROVEEDOR POR VICIOS OCULTOS

El Proveedor es responsable por la calidad ofrecida y por los vicios ocultos de los servicios ofertados por un plazo de dos (02) años contados a partir de las conformidades otorgadas por cada entregable por el Banco de la Nación.

29. REQUISITOS DE CALIFICACIÓN

Tabla 23: Cuadro de Requisitos de Calificación

A	**CAPACIDAD TÉCNICA Y PROFESIONAL**
A.1	**CALIFICACIONES DEL PERSONAL CLAVE**
A.1.1	**FORMACIÓN ACADÉMICA**
	Requisitos: Un (01) Gerente de Proyecto Se requiere Título Universitario en Ingeniería de Sistemas y/o Ingeniería de Cómputo y/o Ingeniería Informática y/o Ingeniería de Telecomunicaciones y/o Ingeniería Industrial y/o Ingeniería Electrónica y/o Administración o afines (*). Tres (03) Especialista de Nube Se requiere como mínimo grado de Bachiller en Ingeniería de Sistemas y/o Ingeniería de Cómputo y/o Ingeniería Informática y/o Ingeniería de Telecomunicaciones y/o Ingeniería Industrial y/o Ingeniería Electrónica o afines (*). **(*):**El párrafo "o carrera, afines a tecnología de la información" se refiere a cualquiera de las carreras listadas a continuación: Ingeniería de Sistemas, Ingeniería Informática, Ingeniería Industrial, Ingeniería Electrónica, Ingeniería de Computación y Sistemas, Ingeniería de Telecomunicaciones, Ingeniería Industrial y de Sistemas, Ingeniería de Sistemas e Informática, Ingeniería de Sistemas Empresariales, Ingeniería de Software , Ingeniería de Sistemas de Información, Ingeniería de Telecomunicaciones y Redes,

	Ingeniería de Computación y de Sistemas, Ingeniería Informática y de Sistemas, Ingeniería de Redes y Comunicaciones, Ingeniería de Seguridad Informática, Ingeniería Empresarial y de Sistemas, Ingeniería de Estadística e Informática, Ingeniería de Sistemas y Cómputo, Ingeniería de Sistemas e Informática, Ingeniería Empresarial, Computación e Informática, Ingeniería de Computación, Licenciado (a) en Computación, Ingeniería de Sistemas y Computación, Ciencias de la Computación, Ciencias de la Información, Licenciado (a) Administración y Sistemas. **Acreditación:** El Grado de Bachiller o Título serán verificado por el comité de selección en el Registro Nacional de Grados Académicos y Títulos Profesionales en el portal web de la Superintendencia Nacional de Educación Superior Universitaria - SUNEDU a través del siguiente link: https://enlinea.sunedu.gob.pe/ // o en el Registro Nacional de Certificados, Grados y Títulos a cargo del Ministerio de Educación a través del siguiente link: http://www.titulosinstitutos.pe/, según corresponda. Nota: El postor debe señalar los nombres y apellidos, DNI y profesión del personal clave, así como el nombre de la universidad o institución educativa que expidió el grado requerido. En caso de que el Grado de Bachiller o Título profesional no se encuentre inscrito en el referido registro, el postor debe presentar la copia del diploma respectivo a fin de acreditar la formación académica requerida.
A.1.2	**CAPACITACIÓN**
	Requisitos: Un (01) Gerente de Proyecto • Diplomado en Gerencia de Proyectos bajo enfoque PMI o Certificación PMP del Project Management Institute[17]. Tres (03) Especialistas de Nube: Cada especialista deberá cumplir con al menos uno de los puntos, pero en conjunto, los tres especialistas deberán tener los tres puntos solicitados. • Certificado oficial o curso completado en arquitectura Cloud de nivel profesional de la marca de la nube a ofertar[18]. • Certificado oficial o curso completado en seguridad Cloud[19] de nivel profesional o asociado de la marca de la nube a ofertar. • Certificación o curso completado en DevOps. **Acreditación:** Se acreditará con copia simple de Certificados o Constancias que demuestren fehacientemente la capacitación requerida afines al presente requerimiento[20].
A.2	**EXPERIENCIA DEL PERSONAL CLAVE**
	Requisitos: Un (01) Gerente de Proyecto • Deberá acreditar experiencia mínima de cinco (05) años como Project Manager o jefe de proyecto y/o implementación de Soluciones de Servicios en Nube y/o mantenimiento o Soporte Cloud.

[17] Pliego de Consultas N° 01-2024 - Concurso de Méritos (Consulta N° 62 TCO LATAM).
[18] Pliego de Consultas N° 01-2024 - Concurso de Méritos (Consulta N° 63 TCO LATAM).
[19] Pliego de Consultas N° 01-2024 - Concurso de Méritos (Consulta N° 63 TCO LATAM).
[20] Pliego de Consultas N° 01-2024 - Concurso de Méritos (Consulta N° 51 TCO LATAM).

	Tres (03) Especialistas de Nube • Deberá acreditar experiencia mínima de tres (03) años en desarrollo y/o arquitectura y/o implementación y/o configuración y/o instalación de soluciones en nube o soluciones de Cloud o soluciones de Cloud Computing o infraestructura en nube. • Deberá acreditar experiencia mínima de dos (02) años en arquitectura y/o implementación y/o supervisor y/o configuración y/o instalación de desarrollo en nube o soluciones de cloud o soluciones de cloud computing o infraestructura en nube. • Experiencia mínima de tres (3) años realizando implementación de servicios de seguridad en nube • Experiencia mínima de dos (2) años realizando implementación de servicios DevOps. **Acreditación:** La experiencia del personal clave se acreditará con cualquiera de los siguientes documentos: (i) copia simple de contratos y su respectiva conformidad o (ii) constancias o (iii) certificados o (iv) cualquier otra documentación que, de manera fehaciente demuestre la experiencia del personal propuesto.
B.	**EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD**
	Requisitos: a) El postor debe acreditar un monto facturado acumulado equivalente de diez millones y 00/100 Soles (S/ 10,000,000.00), por la contratación de servicios iguales o similares al objeto de la convocatoria, durante los ocho (08) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda. La experiencia debe estar orientada al sector financiero y, de manera opcional, abarcar un alcance global. b) Se consideran servicios similares a los siguientes: • Servicio de consultoría en la gestión de proyectos con metodologías ágiles. • Servicios de implementación de mesas o células ágiles en el sector financiero. • Servicio de consultoría en sistemas informáticos bancarios en entidades financieras • Servicio de consultoría en análisis UX / UI • Servicio de implementación en entornos nube en entidades financieras • Servicios de desarrollo e implementación de aplicaciones móviles financieras • Servicios de desarrollo e implementación de aplicaciones móviles • Servicios de desarrollo e implementación de aplicaciones móviles bancarias • Servicios de desarrollo e implementación de portales web para el sector financiero • Servicios de desarrollo e implementación de banca digital por internet o Homebanking • Experiencia comprobada en servicios de implementación y despliegue en nubes, trabajando con al menos dos (02) fabricantes reconocidos en el mercado a nivel mundial.

	Acreditación: Se acreditará con copia simple de (i) contratos u órdenes de servicios, y su respectiva conformidad o constancia de prestación; o (ii) comprobantes de pago cuya cancelación se acredite documental y fehacientemente, con voucher de depósito, nota de abono, reporte de estado de cuenta, cualquier otro documento emitido por Entidad del sistema financiero que acredite el abono o mediante cancelación en el mismo comprobante de pago, correspondientes a un máximo de veinte (20) contrataciones.

- **Documentos para presentarse a la suscripción del contrato**

  Carta u otro documento oficial que acredite la condición de "partner" con una empresa que brinda servicios en la nube, concordante con el numeral 9. Arquitectura Tecnológica Requerida de los TDR.

30. SEGURIDAD Y SALUD EN EL TRABAJO

El ganador de la Buena PRO a la suscripción del contrato deberá presentar obligatoriamente una Declaración Jurada que cumple las disposiciones establecidas en la Ley N° 29783 - Ley de Seguridad y Salud en el Trabajo y su Reglamento.

31. PREVENCIÓN DEL LAVADO DE ACTIVOS Y DEL FINANCIAMIENTO DEL TERRORISMO

A la suscripción del contrato, el ganador de la buena pro debe presentar la siguiente Información:

- Nombres y Apellidos completos o denominación o razón social, el caso se trate de una persona jurídica.
- Registro Único de Contribuyentes (RUC), o registro equivalente para no domiciliados, de ser el caso.
- Tipo u número de documento de Identidad, en caso de trate de una persona natural.
- Dirección de la oficina o local principal.
- Años de Experiencia en el mercado.
- Rubros en los que el proveedor brinda sus productos o servicios.
- Identificación de los accionistas, socios o asociados que tengan directa o indirectamente el 25 % del capital social, aporte o participación de la persona jurídica y del nombre del representante legal, considerando la información requerida para las personas naturales.
- Declaración Jurada de no contar con antecedentes penales del proveedor, de ser el caso.
- No encontrarse incluido en la lista emitida por la Oficina de Control de Activos Extranjeros del Departamento de Tesoro de los Estados Unidos de América (OFAC).

De acuerdo con el Anexo N° 1 de la Resolución S.B.S. N° 2660-2015 Reglamento de Gestión de Riesgos de Lavado de Activos y del Financiamiento del Terrorismo, el proveedor adjudicado con la buena pro deberá cumplir con lo

especificado por dicha Resolución, lo cual será verificado por el Banco antes de la firma del contrato.

32. REGISTRO DE DEUDORES DE REPARACIÓN CIVIL - REDERECI

A la suscripción del contrato, el ganador de la buena pro debe presentar Declaración Jurada de no encontrarse inscritos en el Registro de Deudores de Reparación Civil.

33. SERVICIO DE ASISTENCIA PARA ALCANZAR LA MEJORA CONTINUA DE LA SOLUCIÓN

Con el objetivo de garantizar el éxito continuo y la eficiencia operativa de la solución tecnológica se solicita la contratación de Servicio de Asistencia para Alcanzar la Mejora Continua de la Solución, el servicio tendrá la modalidad bajo demanda durante el tiempo de ejecución del contrato.

El inicio del servicio de Mejora Continua empezará al día siguiente de la suscripción del Acta de Conformidad correspondiente al MVP 4.

a Mejora Continua:
- Revisiones regulares del rendimiento de las soluciones implementadas.
- Identificación de oportunidades de optimización y eficiencia.
- Implementación de actualizaciones y mejoras según sea necesario.
- Integración con nuevas herramientas y/o versiones de los sistemas antifraudes para operaciones financieras y no financieros disponibles en el Banco.
- Implementación de encuestas cortas de satisfacción de la experiencia del usuario mediante el administrador de contenidos, los cuales deberán ser parametrizables.

b Servicio de Mejora Continua bajo Demanda:
- El inicio del servicio nace con un requerimiento por parte del Banco en el cual expresa la necesidad de un nuevo desarrollo o una nueva actualización en para la Banca Móvil y la Banca por Internet, dicho documento debe ser entregado al Contratista para su evaluación y cotización correspondiente.
- El Contratista tendrá un plazo máximo de 5 días calendarios de trabajo para emitir su cotización, a la cual debe anexar: cronograma de trabajo, presupuesto, equipo de trabajo, metodología de desarrollo y demás documentos que el Contratista considere pertinente.
- Dicha cotización será recibida por el Banco y será evaluará en un plazo máximo de 7 días hábiles.
- De existir observaciones por parte de Banco, el Contratista tendrá un plazo de 5 días calendarios para levantar las consultas.
- Una vez que la cotización este aprobada por la subgerencia de Innovación Digital, se le hará llegar al Contratista para su conocimiento
- Recibida la orden, el Contratista tendrá un plazo máximo de 15 días calendarios para iniciar el desarrollo del servicio.
- Al finalizar este período, se evaluará la posibilidad de renovación, sujeto a revisión de desempeño y necesidades en evolución.

c Informes y Entregables:

- Entrega de informes detallados sobre el soporte proporcionado.
- Se respetará la misma metodología de gestión de proyectos del presente requerimiento, descritos en el numeral 20. Obligaciones del Contratista.

d Penalidades del servicio de Mejora Continua
- El Banco tendrá la potestad de desestimar el proceso de contratación si el Contratista no cumple con las fechas establecidas en la modalidad de bajo demanda del servicio de Mejora Continua.
- Una vez emitida y aceptada la orden de servicio y existir retrasos en el inicio del servicio, el Banco aplicará las penalidades por mora descritas en el numeral 35.1 Penalidad por Mora.

e Recurso de personal de mejora continua (ver numeral 26.3 Recurso de Personal para la Mejora Continua del Servicio)

f La Formación Académica, capacitación y experiencia exigida para el personal no clave requeridos en el numeral 26. Recursos de Personal del Contratista para la mejora continua del servicio, deberá ser acreditado por el postor adjudicado con la buena pro, a la suscripción del contrato con la presentación de la documentación que acredite las condiciones establecidas.

g El Contratista se compromete a no reasignar ni remover ningún miembro de su personal asignado al servicio de Mejora Continua, sin la aprobación del Banco de la Nación durante.

h El Banco de la Nación podrá solicitar al Contratista el reemplazo de miembros de su personal, comprometiéndose el Contratista a asignar personal de calificaciones similares o superiores al(los) miembro(s) a ser reemplazado(s). De aplicarse este caso, el Contratista debe reemplazar al personal en un plazo máximo de tres (3) días calendario, después de la aprobación realizada por el BN a través de correo electrónico.

i De producirse un reemplazo de algún personal por motivo de fuerza mayor, el Contratista comunicará la salida del personal con un plazo máximo de 24 horas de ocurrido el evento y deberá realizar el reemplazo, en un plazo máximo de tres (3) días calendario. Se indica que el personal reemplazante debe tener igual o superior perfil que el reemplazado y deberá contar con la aprobación del Bando de la Nación.

34. PROPIEDAD INTELECTUAL (DERECHOS DE AUTOR)

El proveedor adjudicado cede en forma ilimitada, exclusiva y gratuita:

- Todos los derechos patrimoniales y formas de explotación reconocidos por el Decreto Legislativo N° 822, Ley sobre Derechos de Autor, relativos a los sistemas del Banco de la Nación, objeto del presente contrato.
- Todos los derechos sobre la documentación y los entregables que realice y produzca a favor del Banco de la Nación como consecuencia del proyecto que se le encargue.

Dichos derechos serán libremente ejercidos y explotados sin restricción por el Banco de la Nación, pudiendo éste realizar modificaciones o versiones sucesivas del software materia del presente contrato y obtener por ello beneficios salvo en los

casos en que se trate de propiedad intelectual del postor incluir las licencias de software la cuales deberán estar a nombre del Banco de la Nación y entregadas en el formato oficial del fabricante, para dar la conformidad de la entrega, la misma que será verificada por el área técnica especializada o por el área usuaria del Banco de la Nación.

En tal sentido, el postor está prohibida directa o indirectamente a través de terceros de: reproducir parcial o totalmente, comunicar al público, reutilizar, distribuir, transformar o aplicar cualquier otra forma distinta a las indicadas en los dos primeros puntos, utilizar los diseños, código fuente, y en general el sistema objeto del contrato, sin expresa y previa autorización del Banco de la Nación.

Esta prohibición tiene vigencia ilimitada, aun cuando el proyecto materia del contrato haya culminado o el contrato haya sido resuelto.

El Banco de la Nación tiene el derecho expedito de realizar las gestiones de inscripción correspondientes ante la Dirección de Derechos de Autor de INDECOPI.

El postor no podrá hacer referencia sobre el Banco de la Nación en publicidad o literatura sin la previa aprobación escrita de éste. Esta prohibición es a perpetuidad y se mantiene vigente aun cuando el contrato haya culminado o haya sido resuelto.

El desarrollo de software, el código fuente generado, y las aplicaciones elaboradas por el postor serán de propiedad del Banco de la Nación.

35. PENALIDADES DEL SERVICIO

35.1. Penalidad por Mora

- En caso de retraso injustificado del Contratista en la ejecución de los entregables respecto a la contratación (ver numeral 16. Entregables), el Banco le aplica automáticamente una penalidad por demora en cada día de atraso sobre el monto total correspondiente a dicho entregable.
- La penalidad se aplica automáticamente y se calcula de acuerdo con la siguiente fórmula:
  - Penalidad diaria = $\frac{0.10 \times \text{monto vigente de la fase}}{F \times \text{plazo vigente en días}}$

    Donde F tiene los valores siguientes:
  - F = 0.25

- Cabe precisar que la penalidad por mora y otras penalidades pueden alcanzar cada una un monto máximo equivalente al diez por ciento (10%) del monto del contrato vigente correspondiente del desarrollo, después del cual el Banco podrá resolver el contrato por incumplimiento.
- En el caso de entregables incompletos, se considerarán como no presentados y empezará a computar el plazo de la penalidad correspondiente.
- La penalidad establecida en la presente cláusula se aplicará sin perjuicio de la obligación del Contratista de responder por los daños y perjuicios que pudieran derivarse de su incumplimiento o de las más sanciones que pudieran corresponder.

- En caso de que el entregable tenga una variación en el alcance que implique la modificación del cronograma, deberán ser sustentados debidamente mediante documentos aprobados por el área técnica y el área usuaria.
- El proceso de alegación será coordinado entre el proveedor de la buena pro del concurso de méritos y el Banco, de acuerdo a la normativa vigente.

35.2. Otras Penalidades

Las penalidades serán aplicadas a aquellas incidencias imputables al proveedor.

- **Penalidad por sustitución del personal profesional**

  Cualquier cambio deberá ser comunicado al Banco, si el Contratista cambia alguno(s) de los profesionales del personal propuesto sin autorización del Banco de la Nación se le aplicará una penalidad de una (01) UIT; la cual será deducida en el periodo de pagos en que se haya observado el incumplimiento.

Las penalidades serán aplicadas luego de transcurrido el plazo establecido para solucionar posibles contingencias de acuerdo con lo señalado en los presentes términos de referencia.

- **Penalidad por atención de incidencias**

Tabla 24: Penalidad por atención de incidencias

Penalidades			
N°	**Supuestos de aplicación de Penalidad**	**Forma de Cálculo**	**Procedimiento**
1. Atención de Incidentes por nivel			
1.1	**Crítica**	La atención supera 30 minutos, se le aplicara 0.5 de una UIT	Informe de la Subgerencia de Producción sobre el incumplimiento del horario de atención
1.2	**Alta**	La atención supera 1 hora, se le aplicara 0.4 de una UIT	
1.3	**Media**	La atención supera 2 horas, se le aplicara 0.3 de una UIT	
1.4	**Baja**	La atención supera 4 horas, se le aplicara 0.2 de una UIT	
2. Solución del incidente por nivel			
2.1	**Crítica**	La atención supera 1 hora, se le aplicara 0.5 de una UIT	Informe de la subgerencia de producción o de la Oficina de Seguridad informática sobre el incumplimiento del tiempo de solución
2.2	**Alta**	La atención supera 2 horas, se le aplicara 0.4 de una UIT	
2.3	**Media**	La atención supera 4	

		horas, se le aplicara 0.3 de una UIT	
2.4	**Baja**	La atención supera 24 horas, se le aplicara 0.2 de una UIT	
3. Entrega de Informe de Remediación por nivel de incidente			
3.1	**Crítico**	La atención supera 10 días, se le aplicara 0.5 de una UIT	Informe de la subgerencia de producción o la Oficina de Seguridad Informática sobre el incumplimiento del tiempo de entrega de informe de remediación.
3.2	**Alta**	La atención supera 12 días, se le aplicara 0.4 de una UIT	
3.3	**Media**	La atención supera 14 días, se le aplicara 0.3 de una UIT	
3.4	**Baja**	La atención supera 16 días, se le aplicara 0.2 de una UIT	

- **Penalidades por Interrupción del Servicio**

Tabla 25: Penalidades por Interrupción del Servicio

Descripción	Penalidad	Base de Cálculo	Procedimiento
Interrupción del servicio de nube por cada 5 minutos acumulados en el mes	0.5	UIT	La Subgerencia de Producción informará las ocurrencias de manera mensual sobre los minutos de servicio de nube interrumpidos mensualmente y el monto será ejecutado de la facturación mensual del servicio de infraestructura.
Interrupción del servicio de seguridad cada 5 minutos acumulados en el mes	0.5	UIT	La Subgerencia de Producción informará las ocurrencias de manera mensual sobre los minutos de servicio de seguridad interrumpidos mensualmente y el monto será ejecutado de la facturación mensual del servicio de seguridad.
Interrupción del servicio de aplicaciones cada 5 minutos acumulados en el mes	0.5	UIT	La Subgerencia de Producción informará las ocurrencias de manera mensual sobre los minutos de servicio de aplicaciones interrumpidos mensualmente y el monto será ejecutado de la facturación mensual del servicio de soporte y mantenimiento.

			Esta penalidad no aplicará si verifica que existe una falla en el servicio de nube como origen del incidente

Cabe precisar que la penalidad por mora y otras penalidades pueden alcanzar cada una un monto máximo equivalente al diez por ciento (10%) del monto del contrato vigente, después del cual el Banco podrá resolver el contrato por incumplimiento.

36. CLAUSULA DE CONTINUIDAD DEL NEGOCIO

EL PROVEEDOR debe desarrollar la gestión de continuidad para el servicio objeto del contrato, mediante la aplicación de la Resolución S.B.S N° 877-2020 Reglamento para la gestión de la continuidad del negocio o buenas prácticas para en la Gestión de Continuidad del Negocio (ISO 20301) para este tipo de servicio.

EL PROVEEDOR se compromete a mantener la continuidad del servicio contratado por EL BANCO; para lo cual, debe contar con procedimientos documentados que permitan responder, recuperar, reanudar y restaurar el servicio objeto del contrato; además, los referidos procedimientos deben formar parte de un Plan de Recuperación de Tecnología de Información o en su defecto de un Plan de Continuidad de Negocio, de tal modo que su ejecución asegure la alta disponibilidad y recuperación del servicio conforme al tiempo objetivo de recuperación (ambos tiempos definidos en numeral 7.1 literales "u" y "v").

EL PROVEEDOR debe entregar a EL BANCO: el Plan de Recuperación de Tecnología de Información / Plan de Continuidad de Negocio, los cuales deban estar actualizados y probados cuando menos una vez al año; asimismo, EL PROVEEDOR deberá contar con un Programa de Pruebas el cual deberá tener procedimientos documentados. Al respecto, EL PROVEEDOR deberá cumplir con lo establecido en el numeral 9.5.2. Servicio con Alta Disponibilidad remitiendo el Plan(es) y Programa de Pruebas, así como un reporte que resuma los resultados alcanzados de las pruebas efectuadas.

EL PROVEEDOR programará las pruebas en coordinación con el Banco a fin de reducir la afectación del servicio; para casos de pruebas que implique la interrupción del servicio, estas deben ser identificadas y comunicadas desde su programación. Dichas pruebas deben contemplar la validación de alta disponibilidad de los componentes que forman parte del servicio, ante una interrupción. Asimismo, EL BANCO podrá solicitar su participación en el desarrollo de dichas pruebas, y de tener alguna observación sobre los resultados de las pruebas podrá remitirla a EL PROVEEDOR para que lo evalúe y responda en un periodo no mayor a treinta (30) días con un plan de acción y fecha estimada para subsanar la(s) observación(es).

Ante la eventual interrupción del servicio objeto del contrato; por causales imputables a EL PROVEEDOR, siempre que dicha interrupción sea por un tiempo mayor a cinco (05) minutos; EL PROVEEDOR deberá comunicar a EL BANCO de forma inmediata o máximo cuatro horas después del incidente que origino la

interrupción la cual debe incluir la hora de inicio y fin caso que el incidente se encuentre superado y posterior deberá remitir un informe de la incidencia, la cual debe contener como mínimo la fecha, hora, duración, causa/origen, responsabilidad, estado de los servicio(s) afectado(s), descripción del incidente, acciones de recuperación realizadas ,diagnostico general, impacto del servicio, acción de mejora y recomendaciones, conclusiones, en un plazo máximo de tres (03) días hábiles, para su reporte se contabiliza a partir de la ocurrencia del evento. En caso de que no se haya concluido las acciones de superen o implementen las recomendaciones estas deberán reportarse hasta que se encuentre superada.
Para casos que EL PROVEEDOR realice cambios a sus configuraciones u otros componentes que involucren/afecten la operatividad del servicio objeto del contrato, deben ser comunicados a EL BANCO con diez (10) días hábiles de anticipación a la Gerencia de Tecnología de la Información para su revisión y aprobación.
EL PROVEEDOR se compromete a entregar a EL BANCO toda la documentación y/o información que pueda ser necesaria para el correcto funcionamiento del servicio objeto del contrato y que además permita a EL BANCO tener un nivel de independencia en sus mantenimientos y mejoras, así como mantener una operación adecuada.

37. SEGURIDAD DE LA INFORMACIÓN Y CIBESEGURIDAD

- Para garantizar la integridad, disponibilidad, confidencialidad y privacidad de la información El CONTRATISTA debe cumplir con los lineamientos de seguridad de la información y ciberseguridad aplicables al servicio contratado, establecidos en las siguientes normativas:

  - **Resolución SBS N.º 504-2021, que aprueba el "Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad".**

    El CONTRATISTA se obliga a adoptar las medidas necesarias para que sus trabajadores, representantes y terceros que intervienen en el servicio contratado, cumplan con las disposiciones relacionadas a la seguridad de información y ciberseguridad establecidas en la normativa interna del Banco.
    El CONTRATISTA es el responsable del resguardo y protección de los activos de información (equipos, dispositivos informáticos, aplicaciones, información, entre otros) de propiedad del Banco de la Nación, involucrados en el servicio contratado, que se encuentren bajo la administración del CONTRATISTA o formen parte de dicho servicio.
    El CONTRATISTA, previo a la puesta en producción del servicio contratado, debe evidenciar que cuenta con las certificaciones ISO/IEC 27001, ISO/IEC 27017 e ISO/IEC 27018, y que cuenta con un reporte SOC 2 tipo 2 u otros equivalentes relevantes al servicio contratado y posterior a la puesta en producción del servicio, debe evidenciar anualmente la vigencia de dichas certificaciones. El CONTRATISTA debe

proporcionar al BN, copia o indicar el enlace web donde se visualicen las referidas certificaciones.
El CONTRATISTA permitirá, facilitará y/u otorgará al Banco la revisión del cumplimiento de las medidas de seguridad de la información relacionadas al servicio contratado.
El CONTRATISTA debe proporcionar las especificaciones técnicas de configuración de las API utilizadas para la provisión del servicio, de ser el caso, de forma que facilite su documentación, auditoría y uso, dicha información debe ser proporcionada al Banco.
El CONTRATISTA declara que tiene pleno conocimiento respecto que EL BANCO se encuentra sujeto a las exigencias de la Resolución SBS N°504- 2021 "Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad" - SUBCAPÍTULO III – AUTENTICACIÓN; por lo que El CONTRATISTA se compromete a implementar en sus sistemas de información los requerimientos del proceso de autenticación asociado al enrolamiento de los usuarios y la autenticación reforzada, que defina EL BANCO.

- **Norma Técnica Peruana NTP- ISO/IEC 27001-2022 – Seguridad de la Información, Ciberseguridad y Protección de la Privacidad. Sistemas de Gestión de la Seguridad de la Información. Requisitos.**

  El CONTRATISTA debe contar con un proceso de gestión de riesgos, alertas e incidentes de seguridad de la información, relacionados con el servicio contratado. Las evidencias de la existencia y ejecución de dicho proceso deben ser remitido al inicio del servicio o a solicitud del Banco.
  El CONTRATISTA, comunicará al Banco cualquier cambio a realizar en los sistemas tecnológicos asociados al servicio contratado. El CONTRATISTA coordinará con el Banco a fin de definir las acciones pertinentes para dicha actividad.
  El CONTRATISTA se obliga a cumplir con los controles de seguridad de la información y ciberseguridad establecidos por el Banco, respecto al control de los accesos, cifrado de la información, la revisión del desempeño, el seguimiento de la ejecución del servicio, presentación de informes y auditorías, así como las obligaciones regulatorias enmarcadas en los requisitos de seguridad de la información.

- Sin perjuicio a lo anterior, en un consocio la empresa que realice el procesamiento, almacenamiento y transmisión de la información del servicio Banca Móvil y Banca por Internet, debe evidenciar que cuenta con las certificaciones ISO/IEC 27001, ISO/IEC 27017 e ISO/IEC 27018, y que cuenta con un reporte SOC 2 tipo 2 u otros equivalentes relevantes al servicio

contratado y posterior a la puesta en producción del servicio, debe evidenciar anualmente la vigencia de dichas certificaciones.

38. CONFIDENCIALIDAD DE LA INFORMACIÓN

- EL BANCO es propietaria de toda la información confidencial que, por razones del alcance del presente contrato, entregue a EL CONTRATISTA.
- El CONTRATISTA se compromete a mantener la confidencialidad y reserva absoluta y a no revelar a terceros, sin previa autorización escrita del Banco, toda información a la que tenga acceso, que le sea suministrada o conozca directa o indirectamente durante la ejecución del servicio contratado.
- El compromiso de confidencialidad se prolonga hasta por 10 años después de terminado el servicio y se hace extensivo al personal de EL CONTRATISTA aun cuando hayan dejado de tener vínculo laboral con EL CONTRATISTA.
- Para los efectos del presente acuerdo, se entenderá como "Información Confidencial" toda aquella información comercial, financiera, técnica, de inteligencia comercial, metodologías, procesos, políticas, procedimientos, estándares, estrategias, productos, bases de datos, matrices y programas de cómputo, código, nombres y/o experiencia de empleados y consultores, propiedad intelectual, fórmulas, negocios, lista de clientes, estados financieros, información sobre productos de software y hardware de EL BANCO, que sea entregada a EL CONTRATISTA, ya sea de manera escrita, oral, visual y/o digital; que por sus características le signifique a EL CONTRATISTA obtener y mantener una ventaja competitiva o económica frente a terceros en la realización de actividades económicas.
- Toda información confidencial, utilizada y custodiada por EL CONTRATISTA para la provisión del servicio contratado, deberá ser devuelta a EL BANCO en un plazo no mayor a diez (10) días calendarios, así como la eliminación de la información ante la culminación del servicio.
- EL CONTRATISTA está autorizado para que su personal pueda hacer uso de la información confidencial provista por EL BANCO siempre que dicho personal esté directamente relacionado a la ejecución del presente contrato, haya sido informado de la naturaleza confidencial del mismo y haya sido instruido sobre las medidas de protección adoptadas por EL CONTRATISTA, las cuales deberá aplicar para la protección de la confidencialidad de esta. EL CONTRATISTA será responsable por las infracciones comprobadas de incumplimiento del acuerdo de confidencialidad que hayan sido cometidas por el personal asignado para la ejecución del servicio objeto del presente Contrato.
- El CONTRATISTA no debe capturar, utilizar, almacenar, acceder, visualizar ni desviar la información de los clientes y usuarios de El BANCO, sin la autorización expresa de El BANCO.

39. PROTECCIÓN DEL SECRETO BANCARIO, TELECOMUNICACIONES, DATOS PERSONALES Y DELITOS INFORMATICOS

- El BANCO y El CONTRATISTA declaran conocer que están obligados a salvaguardar y mantener la confidencialidad del secreto bancario, de las

telecomunicaciones y de los datos personales de los usuarios y clientes del Banco de la Nación, de acuerdo con la Constitución Política del Perú, Ley N°29733 Ley de Protección de datos personales, su Reglamento y Directivas de Seguridad, Ley N°26702, Secreto Bancario y la Ley N° 26096 Ley de Telecomunicaciones, sus modificatorias y actualizaciones; aplicables a los productos o servicios asociado al contrato.

- Del Flujo Transfronterizo: En caso exista flujo transfronterizo de datos personales asociado al servicio contratado, EL CONTRATISTA deberá comunicar a El BANCO y asegurarse que la información de datos personales que se transmita y/o transfiera entre el Perú y cualquier otro país, a causa directa o indirecta del servicio contratado; mantiene y mantendrá los niveles de protección adecuados, disponiendo las medidas de seguridad, privacidad y confidencialidad necesarias y efectivas para evitar la adulteración, pérdida, consulta o tratamiento no autorizado de los datos, y que permitan detectar desviaciones, intencionales o no, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado; verificando que todas estas medidas y acciones no sean inferiores a las dispuestas por la Ley N° 29733, su reglamento, directiva de seguridad y normas conexas, de manera tal que garanticen el nivel de seguridad apropiado para abordar los riesgos asociados al tratamiento de datos personales y a la naturaleza sensible de los datos que han de protegerse. En caso EL BANCO proporcione a EL CONTRATISTA datos personales de sus clientes o usuarios y éste último deba recopilarlos o generarlos, en el marco del cumplimiento del contrato, ello no implicará de modo alguno la transferencia de los mismos, debiendo EL CONTRATISTA asumir en dichos casos, la condición de encargado del tratamiento. EL CONTRATISTA declara conocer que asume la condición de encargado del tratamiento cuando EL BANCO entrega o pone a disposición de manera directa o indirecta a EL CONTRATISTA información que contiene datos personales en virtud de una relación jurídica que los vincula.
- EL CONTRATISTA declara conocer las sanciones tipificadas en la Ley N° 30096, Ley de Delitos Informáticos (integridad de datos informáticos, tráfico ilegal de datos, interceptación de datos informáticos), y la Ley N° 30171 que modifica la Ley 30096, Ley de Delitos Informáticos, bajo la cual se obliga a dar estricto cumplimiento de estas.

40. CLAUSULA DE GESTIÓN INTEGRAL DE RIESGOS Y AUDITORIA

- El proveedor está obligado a permitir la revisión, supervisión e inspección de los servicios prestados y de las condiciones que garanticen la seguridad de información, protección de datos personales, continuidad del negocio y gestión de sus riesgos, por parte de la dependencia responsable del contrato, el Órgano de Auditoría Interna del Banco, de la sociedad auditora externa, así como por parte de la Superintendencia, en la oportunidad que cualquiera de estos órganos lo solicite, con un aviso previo por escrito de veinticuatro (24) horas, el cual será remitido a la dirección indicada por el proveedor en el contrato. En dicho comunicado se designarán a las personas que efectuarán la mencionada revisión, supervisión e inspección. Consecuentemente, el proveedor se

compromete a facilitar todos los recursos y medios necesarios a las personas antes mencionadas para efectuar dicha revisión.

- El Banco asumirá los costos por auditoría interna y auditoría externa.
- El incumplimiento de las obligaciones que asume el proveedor en las cláusulas referidas, constituyen causal de resolución automática y de pleno derecho del presente contrato, de conformidad con lo previsto en el Artículo 165° del Reglamento de la Ley N° 30225 "Ley de contrataciones del Estado" (en el caso de contratos dentro del marco de la Ley de Contrataciones), y el artículo N° 14300 del Código Civil, sin perjuicio de la obligación del proveedor de pagar al Banco la indemnización correspondiente.
- En caso el Banco incurriera en costos y/o multas establecidas por parte de un organismo regulador u otro, mediante una resolución o sentencia firme producto de la interrupción y/o algún error o falla en las condiciones de la prestación del servicio por causas imputables al proveedor, éste se hará totalmente responsable de dichas penalidades, asumiendo el importe de las mismas sin reserva ni limitación alguna, Por lo que, el Banco podrá evaluar la aplicación de penalidades o el pago de indemnización mediante las cláusulas de penalidades que correspondan por la no operatividad del servicio, conforme al SLA que haya definido en los Términos de Referencia.

41. CLÁUSULA DE GESTIÓN DE RIESGOS OPERATIVOS

- El proveedor debe aplicar las medidas de control para la gestión de los riesgos operacionales, que sean aplicables al servicio contratado por el Banco; que permita identificar, evaluar, tratar, controlar y monitorear los diversos riesgos asociados a dicho servicio, siendo responsable frente al Banco en caso de la materialización de algún riesgo operativo que, en el marco de la prestación del servicio, afecte al Banco y/o sus clientes.

42. INFORMACIÓN ADICIONAL

- La inclusión de enlaces, logotipos y/o referencias de marcas comerciales ajenas a la institución, deberán ser autorizados expresamente por el Banco de la Nación.
- Es responsabilidad del Contratista asignar los recursos suficientes para el servicio prestado al Banco de la Nación, garantizando el cumplimiento de las actividades y plazos del servicio.
- Después de plazo permitido, una vez implementada el presente proyecto, el Banco podrá, a su discreción, considerar la posibilidad de incorporar al personal especializado del Contratista, siempre y cuando no mantenga ningún vínculo laboral con otra entidad pública o privada.
- El Banco proveerá de especialistas asignados a fin de gestionar, facilitar, verificar los procesos y productos según corresponda en la ejecución del presente proyecto.
- Con relación del punto anterior, a fin de asegurar la continuidad del proyecto, el área correspondiente deberá garantizar de forma ininterrumpida la disponibilidad

de un especialista, incluso en vacaciones, permisos personales, descansos médicos, entre otros.

43. SISTEMA DE CONTRATACIÓN

El sistema de contratación para el servicio de la "Implementación de la nueva plataforma bancaria para los canales digitales Banca Móvil y Banca por Internet del Banco de la Nación" es un **Esquema Mixto de Suma Alzada y Precios Unitarios**. De acuerdo con el siguiente detalle:

43.1. Sistema de Contratación para la Implementación del Proyecto

Concepto	Descripción	Tipo de Esquema mixto
Diseño, Desarrollo e Implementación de la Solución (21.1)	Incluye diseño de interfaz, desarrollo e implementación de las funcionalidades de la Banca Móvil y Banca por Internet descritas en el numeral 7. Alcance y Descripción del Servicio y en el numeral 13. Desarrollo de APIs	**Suma alzada**
Implementación de la Infraestructura (21.2.b.1)	Despliegue base para los ambientes	**Suma alzada**
	Despliegue del ambiente de desarrollo (DEV)	**Suma alzada**
	Despliegue del ambiente de Calidad (QA)	**Suma alzada**
	Despliegue del ambiente de Producción (PRD)	**Suma alzada**
Implementación del Ambiente de Seguridad (21.2.b.2.)	Servicio de implementación Plataforma de protección para aplicaciones CNAPP	**Suma alzada**
	Servicio Implementación Firewall	**Suma alzada**
	Servicio Implementación SaaS de Seguridad para los servicios WAF, ataques volumétricos de denegación de servicio y servicio de seguridad de API discovery	**Suma alzada**
	Servicio Implementación para el Servicio de Detección Avanzada para ataques de Bots Automatizados	**Suma alzada**
Servicio de Soporte Técnico (21.2.b.4.)	Soporte técnico para la atención y resolución de todos los problemas que se presenten con la solución propuesta	**Suma alzada**
Servicio de Asistencia para Alcanzar la Mejora Continua de la Solución (21.2.b.4.)	Tendrá una duración de 90 días calendarios bajo la modalidad de bolsa de trabajo que considera 600 horas mensuales (total del servicio 1,800 horas), terminado el periodo de 90 días, el servicio tendrá la modalidad bajo demanda durante el tiempo de ejecución del contrato.	**Precios unitarios**
	Despues de los 90 días calendarios, el servicio tendrá la modalidad bajo demanda durante el tiempo de ejecución del contrato.	**Precios unitarios**

43.2. Sistema de Contratación para los componentes del Proyecto

Las especificaciones de capacidades siguientes deberán cotizarse para el consumo de Banco de la nación, a no ser que estos servicios de Nube se entreguen en su totalidad en modalidad SaaS 100% gestionada por el contratista a costo fijo, ya sea para los servicios compartidos, los componentes a demanda y para los ambientes de Producción, Certificación (QA) y Desarrollo (Dev).

Ítem	Componente	Tipo de Esquema mixto
10.1. Servicios Compartidos		
1	Componentes del Servicio	**Precio unitario**
2	Servicio de NAT Horas	**Precio unitario**
3	Conexión VPN Site to Site	**Precio unitario**
4	Conexión Cliente VPN	**Precio unitario**
5	Conector de redes en múltiples zonas	**Precio unitario**
6	Servicio de transferencia de datos	**Precio unitario**
7	Kit de desarrollo de software en la nube	**Precio unitario**
8	Servicio de entrega continua	**Precio unitario**
9	Repositorio de paquetes de software	**Precio unitario**
10	Servicio de construcción e integración continua con Sistema operativo Linux.	**Precio unitario**
11	Recurso de cómputo con las siguientes características: 8 vCPU y 16 GB Memoria	**Precio unitario**
12	Registro de contenedores	**Precio unitario**
13	Servicio de autenticación Web/móvil	**Precio unitario**
14	Servicio de logs de la consola en nube	**Precio unitario**
10.2. Ambiente de Producción		
1	Componentes del Servicio	**Precio unitario**
2	Servicio de base de datos relacional compatible con PostgreSQL en alta disponibilidad (Primario/Respaldo) en multizona	**Precio unitario**
3	Cada característica puede consumirse de manera independiente	**Precio unitario**

4	Servicio de base de datos de documentos compatible con (mongoDB) Cada característica puede consumirse de manera independiente 2 Instancias, una por Zona de disponibilidad	**Precio unitario**
5	Servicio de administración y despliegue de APIs	**Precio unitario**
6	Balanceador de carga de red	**Precio unitario**
7	Servicio de contenedores basado en Kubernetes	**Precio unitario**
8	Servicio de máquinas virtuales de cómputo para kubernetes con Sistema operativo Linux	**Precio unitario**
9	Servicio de CDN	**Precio unitario**
10	Servicio de gestión de claves criptográficas	**Precio unitario**
11	Servicio de almacenamiento de secretos	**Precio unitario**
12	Servicio de almacenamiento de objetos	**Precio unitario**
13	Servicio de monitoreo y observabilidad	**Precio unitario**
14	SFTP	**Precio unitario**
15	Servicio de ejecución de Funciones sin servidor	**Precio unitario**
10.3. Ambiente de Certificación (QA)		
1	Componentes del Servicio	**Precio unitario**
2	Servicio de base de datos relacional compatible con PostgreSQL en alta disponibilidad (Primario/Respaldo) en multizona	**Precio unitario**
3	Servicio de base de datos de documentos compatible con (mongoDB) Cada característica puede consumirse de manera independiente 2 Instancias, una por Zona de disponibilidad	**Precio unitario**
4	Servicio de administración y despliegue de APIs	**Precio unitario**
5	Balanceador de carga de de aplicación	**Precio unitario**
6	Servicio de contenedores basado en Kubernetes	**Precio unitario**
7	Servicio de máquinas virtuales de cómputo con Sistema operativo Linux	**Precio unitario**
8	Servicio de CDN	**Precio unitario**
9	Servicio de gestión de claves criptográficas	**Precio unitario**
10	Servicio de almacenamiento de secretos	**Precio unitario**
11	Servicio de almacenamiento de objetos	**Precio unitario**
12	Servicio de monitoreo y observabilidad	**Precio unitario**
13	SFTP	**Precio unitario**
14	Servicio de ejecución de Funciones sin servidor	**Precio unitario**

10.4. Ambiente Desarrollo (DEV)		
1	Componentes del Servicio	**Precio unitario**
2	Servicio de base de datos relacional compatible con PostgreSQL	**Precio unitario**
3	Servicio de base de datos de documentos compatible con (mongoDB) Servicio de administración y despliegue de APIs	**Precio unitario**
4	Balanceador de carga de aplicación	**Precio unitario**
5	Servicio de contenedores basado en Kubernetes	**Precio unitario**
6	Servicio de máquinas virtuales de cómputo con Sistema operativo Linux	**Precio unitario**
7	Servicio de CDN	**Precio unitario**
8	Servicio de gestión de claves criptográficas	**Precio unitario**
9	Servicio de almacenamiento de secretos	**Precio unitario**
10	Servicio de almacenamiento de objetos	**Precio unitario**
11	Servicio de monitoreo y observabilidad	**Precio unitario**
12	SFTP	**Precio unitario**
13	Servicio de ejecución de Funciones sin servidor	**Precio unitario**
10.5. Componentes a Demanda		
1	Servicio de base de datos relacional (HA)	**Precio unitario**
2	Servicio de base de datos de documentos	**Precio unitario**
3	Servicio de máquinas virtuales de cómputo para kubernetes con Sistema operativo Linux	**Precio unitario**
4	Direct Connet hosteado	**Precio unitario**
11.8. Especificaciones de Capacidades de los Servicios de Seguridad		
1	Componentes del Servicio	**Suma alzada**
2	Consola SaaS de Seguridad para los servicios WAF, ataques volumétricos de denegación de servicio y servicio de seguridad de APIs.	**Suma alzada**
3	Plataforma de protección nativa de nube para aplicaciones (CNAPP)	**Suma alzada**
4	Servicio de Next Generation Firewall (NGFW)	**Suma alzada**

43.3. Sistema de Contratación para la integración con Cuenta DNI

Concepto	Escenarios Opcionales	Tipo de Esquema mixto
Cuenta DNI	**Escenario 1:** El contratista deberá realizar el desarrollo correspondiente a fin de enlazar los servicios del APP con los recursos de nube donde se encuentra alojado Cuenta DNI. Se coordinará con el proveedor los accesos correspondientes y las pruebas necesarias.	**Suma alzada**

	Escenario 2: La Cuenta DNI será considerada como una Cuenta BN y el Contratista deberá realizar el desarrollo a fin de dar el mismo tratamiento que a las demás cuentas que se encuentran registradas en el Core Bancario (Mainframe).	**Suma alzada**

Sin embargo, para el concepto cantidad de integraciones y/o incremento de requerimientos de negocio en exceso, corresponderá el sistema de contratación a precios unitarios a través de una cantidad de horas (bolsa de horas) durante la vigencia del contrato, la cual solo se activará a petición del Banco de la Nación y no se cobrará en caso no se use.

Anexos

Anexo N° 1 – Product Backlog

Todos los paquetes definidos en el presente anexo se deberán considerar como un plan de implementación del servicio para la nueva plataforma de la aplicación móvil y Banca por Internet del Banco de la Nación.

1. Product Backlog

MVP	PAQUETES	REFERENCIA
1	**Paquete 0:** Enrolamiento al canal digital (clave de acceso de 6 dígitos y Clave Dinámica Digital)	7.1. Descripción y condiciones del servicio 7.2. Enrolamiento al canal digital 7.3. Enrolamiento a la Cuenta DNI 7.4 Afiliación a la Clave Dinámica Digital (CDD) 7.5 Gestión de Claves Centralizadas
	Paquete 1: Inicio de Sesión	7.6 Recuperación de la contraseña de Internet 7.7 Primer Inicio de Sesión 7.8 Inicio de Sesión del Cliente Recurrente 7.9 Factores de Autenticación y Seguridad del Cliente
	Paquete 2: consulta de productos, saldos y movimientos (página de inicio)	7.10 Consultas de Productos, Saldos y Movimientos
	Paquete 3: Transferencia (Inmediata Mismo Banco)	7.11 Transferencias Bancarias
	Paquete 4: Transferencia (Inmediata Interbancaria)	7.11 Transferencias Bancarias
	Paquete 5: Interoperabilidad (por Número de Teléfono, por QR y por contacto)	7.11 Transferencias Bancarias
	Paquete 6: Retiro Sin Tarjeta de cuentas BN	7.12 Retiro sin tarjeta y por agentes corresponsales
	Paquete 7: Seguridad (Notificaciones, Cambio Clave de Internet, Olvido de clave de internet, Generación de PUSH para validación de transacciones.)	7.13 Módulo de Seguridad
	Paquete 8: Token físico o Clave Dinámica Digital	7.4 Afiliación a la Clave Dinámica Digital (CDD) 7.5 Gestión de Claves Centralizadas 7.13 Módulo de Seguridad
	Paquete 9: Configuración de multidioma (español / quechua)	7.14 Configuración de Multidioma
2	**Paquete 10:** Pago de Servicios y pago a empresas	7.15 Pago de Servicios y pago a empresas
	Paquete 11: Recargas Móviles	7.16 Recargas móviles
	Paquete 12: Actualiza tus Datos (Datos personales)	7.17 Actualización de Datos Personales
	Paquete 13: Transferencias (Diferida)	7.11 Transferencias Bancarias

	Paquete 14: Operaciones Favoritas	7.18 Operaciones Favoritas
	Paquete 15: Giros Nacionales	7.19 Giros Nacionales
	Paquete 16: Bloqueo de Tarjeta de débito y crédito	7.20 Bloqueo de Tarjetas de Débito o de Crédito
3	**Paquete 17:** Pago de Tarjeta de Crédito (del mismo Banco y de otros Bancos)	7.21 Pago de Tarjeta de Crédito
	Paquete 18: Créditos Digitales	7.22 Créditos Digitales
	Paquete 19: Consulta tu Estado de Cuenta (hasta 6 meses)	7.23 Consulta de Estado de Cuenta
	Paquete 20: Ubícanos (Cajeros, Agencias y Agentes)	7.24 Ubicación de Agencias, Cajeros y Agentes
	Paquete 21: Configuración de los atributos de Cuentas y Tarjetas de los clientes	7.25 Configuración de los atributos de Cuentas y Tarjetas de los clientes
4	**Paquete 22**: Módulo de Administración	7.26 Módulo de Administración
	Paquete 23: Avisos Institucionales	7.26 Módulo de Administración
	Enlace 1: Ayuda o Soporte al Cliente	7.26 Módulo de Administración
	Enlace 2: Chat BOT	7.26 Módulo de Administración
	Enlace 3: Págalo.pe	7.27 Pago de Tasas

2. Paquete Opcional

Paquete 24: Cuenta DNI	Este requerimiento tiene como objetivo permitir que los clientes del Banco de la Nación puedan vincular su Cuenta DNI, directamente desde la Banca Móvil y Banca por Internet del Banco. Esto proporcionará a los clientes la capacidad de realizar transacciones digitales y pagos de manera conveniente. Este requerimiento será implementado según la necesidad del Banco.

Anexo N° 2 – Product Backlog para los canales digitales Banca Móvil y Banca por Internet del Banco de la Nación

MVP	PAQUETES	Banca Móvil	Banca por Internet
1	**Paquete 0:** Enrolamiento al canal digital (clave de acceso de 6 dígitos y Clave Dinámica Digital)	Sí	Generación de la clave de internet
	Paquete 1: Inicio de Sesión	Sí	Sí
	Paquete 2: consulta de productos, saldos y movimientos (página de inicio)	Sí	Sí
	Paquete 3: Transferencia (Inmediata Mismo Banco)	Sí	Sí
	Paquete 4: Transferencia (Inmediata Interbancaria)	Sí	Sí
	Paquete 5: Interoperabilidad (por Número de Teléfono, por QR y por contacto)	Sí	Sí Nota: en la Banca por Internet se incluirá la transferencia por contacto
	Paquete 6: Retiro Sin Tarjeta de cuentas BN	Sí	Sí
	Paquete 7: Seguridad (Notificaciones, Cambio Clave de Internet, Olvido de clave de internet, Generación de PUSH para validación de transacciones.)	Sí	Sí
	Paquete 8: Token físico o Clave Dinámica Digital	Sí	Sí
	Paquete 9: Configuración de multidioma (español / quechua)	Sí	Sí
2	**Paquete 10:** Pago de Servicios y pago a empresas	Sí	Sí
	Paquete 11: Recargas Móviles	Sí	Sí
	Paquete 12: Actualiza tus Datos (Datos personales)	Sí	Sí
	Paquete 13: Transferencias (Diferida)	Sí	Sí
	Paquete 14: Operaciones Favoritas	Sí	Sí
	Paquete 15: Giros Nacionales	Sí	Sí
	Paquete 16: Bloqueo de Tarjeta de débito y crédito	Sí	Sí
3	**Paquete 17:** Pago de Tarjeta de Crédito (del mismo Banco y de otros Bancos)	Sí	Sí
	Paquete 18: Créditos Digitales	Sí	Sí
	Paquete 19: Consulta tu Estado de Cuenta (hasta 6 meses)	Sí	Sí

	Paquete 20: Ubícanos (Cajeros, Agencias y Agentes)	Sí	Sí
	Paquete 21: Configuración de los atributos de Cuentas y Tarjetas de los clientes	Sí	Sí
4	**Paquete 22**: Módulo de Administración	No aplica	No aplica
	Paquete 23: Avisos Institucionales	No aplica	No aplica
	Enlace 1: Ayuda o Soporte al Cliente	Sí	Sí
	Enlace 2: Chat BOT	Sí	Sí
	Enlace 3: Págalo.pe	Sí	Sí

1. Paquete Opcional

PAQUETES	Banca Móvil	Banca por Internet
Paquete 24: Cuenta DNI	Sí	Sí

Anexo N° 3 – Componentes Opcionales

Para lo cual, el Contratista deberá considerar la siguiente componente de manera opcional:

Componentes a evaluación	Referencia	Descripción
Gestión de claves centralizadas en la nube	7.5 Gestión de claves centralizadas	Al inicio del proyecto, como piloto, se considera que la centralización de la clave se manejará desde un componente en la nube, que el Contratista deberá proveer e implementar hasta un máximo de 100 usuarios activos y estará activo por 12 meses o hasta la puesta en producción del MVP 4. Posteriormente al MVP 1, el Banco decidirá su permanencia en la nube, cambio o desarrollo de un componente propio del Banco que será creado por el área de TI. Durante la implementación de este MVP 1, se evaluará las prestaciones de este componente, es decir, la performance, seguridad y costos asociados y proyectados según la volumetría futura. En base estos resultados, se podría adoptar este servicio de manera permanente y en caso, esta alternativa no sea elegida, el Banco evaluará los siguientes escenarios opcionales: **Escenario 1:** El desarrollo del módulo de autenticación considerando los mismos criterios de seguridad que mantiene actualmente app y web del BN (generación de clave en mainframe, utilización de los actuales métodos encriptación para las claves, reutilización del proceso actual que utiliza el BN para la generación de la Clave Dinámica Digital). **Escenario 2:** La adquisición de una solución On-Premise que mantenga los mismos estándares de seguridad y de performance del servicio de nube. En ambos escenarios, el Contratista deberá realizar la integración del componente de las Claves Centralizadas con la nueva plataforma de la Banca Móvil y la Banca por Internet.
Cuenta DNI con servicios de nube	7.26 Cuenta DNI	**Escenario 1:** El contratista deberá enlazar los servicios de la Banca Móvil y Banca por Internet con los recursos de Nube (Core Cuenta DNI) donde se encuentra alojado actualmente. Se coordinará con el proveedor los accesos correspondientes y las pruebas necesarias. **Escenario 2:** La Cuenta DNI será considerada como una Cuenta BN y se le dará el mismo tratamiento que a las demás cuentas que se encuentran registradas en el Core Bancario (Mainframe). En ambos escenarios, el Contratista deberá realizar la integración del servicio de Cuenta DNI con la nueva plataforma de la Banca Móvil y la Banca por Internet.

Anexo N° 4 – Integración de la Cuenta DNI

El proveedor ganador de la buena pro será responsable de integrar la nueva plataforma de Banca Digital del Banco de la Nación (BN) con el sistema central (core) de Cuenta DNI, independientemente de si este sistema se encuentra alojado en la nube (cloud) o en las instalaciones físicas del banco (on-premises). Esta integración deberá garantizar la cor recta comunicación y funcionamiento entre la plataforma de Banca Digital y el sistema de Cuenta DNI, permitiendo a los usuarios acceder a los servicios y funcionalidades de Cuenta DNI.

Sin perjuicio a lo anterior, el proveedor adjudicado con la buena pro deberá proponer un (01) diseño diferenciado para la sección de Cuenta DNI considerando los procesos y flujos de las transacciones bancarias aprobados para la cuenta de ahorros BN, es decir que, está cuenta será tratada del mismo modo que las cuentas pasivas del Banco de la Nación, definidos en el numeral 7.1.w.

De llevarse a cabo el desarrollo del componente Cuenta DNI considerado como opcional y a demanda. La ejecución de este desarrollo será comunicada oportunamente al Contratista con al menos 90 días calendarios de anticipación antes de finalizar el MVP 4.

1. Plazo de implementación de Cuenta DNI

El análisis, diseño, desarrollo e implementación del componente Cuenta DNI deberá tener una duración máxima de 150 días calendarios desde la aprobación del Anexo 4.

Actividad	Desde la fecha de confirmación del inicio de ejecución, por parte del Banco
Análisis y diseño UX/UI	45 días
Desarrollo, certificación, pentesting y documentación	90 días
Despliegue en producción	15 días
Total	**150 días**

2. Entregables de la implementación de Cuenta DNI

El proveedor ganador de la buena pro deberá considerar los entregables descritos en el numeral 16. Entregables, para integración de la cuenta DNI.

3. Acta de conformidad de Cuenta DNI

El Acta de Conformidad del Servicio serán emitidas por la Subgerencia Innovación Digital de la Gerencia de Banca Digital como área usuaria y con los informes favorables de las siguientes áreas:

2.1. Informe de las pruebas funcionales de la Sección de Canales Virtuales de la Subgerencia de Canales Alternos y Proyecto Cuenta DNI de la Gerencia de Banca Digital.

2.2. Informe emitido por la Gerencia de Tecnologías de Información que contenga los informes técnicos emitidos por la Subgerencia de Producción, por la Subgerencia de Construcción y por la Oficina de Seguridad Informática.

Dichos documentos serán remitidos a la Sección Ejecución y Seguimiento de Contratos de la Subgerencia de Compras y, comunicará vía correo electrónico al Contratista la emisión de dicho documento.

4. Forma de Pago de la Implementación de Cuenta DNI

El pago correspondiente a la implementación de la Cuenta DNI se realizará una vez que el desarrollo e implementación hayan alcanzado el 100% de culminación, teniendo en cuenta el Ciclo de Vida de Software del Banco de la Nación. Esto se llevará a cabo después de que la Subgerencia de Innovación Digital, como área usuaria, haya emitido el acta de conformidad correspondiente. Además, se requerirá la recepción del informe técnico favorable de la validación por parte de la Gerencia de Tecnologías de la Información, como área técnica.

Anexo N° 5 – Estimación de la Demanda en los Canales Digitales de Clientes del Banco de la Nación

1. Número de Transacciones Proyectadas para el Proyecto

Año	Número de Transacciones por mes promedio
2023	24,000,000*
Año 1	333,333**
Año 2	24,000,000
Año 3	26,400,000

*Fuente: QUIPUS – BN al mes de febrero 2024. Banca Digital – Sección de Canales Alternos (Datos referenciales)
**Número estimado

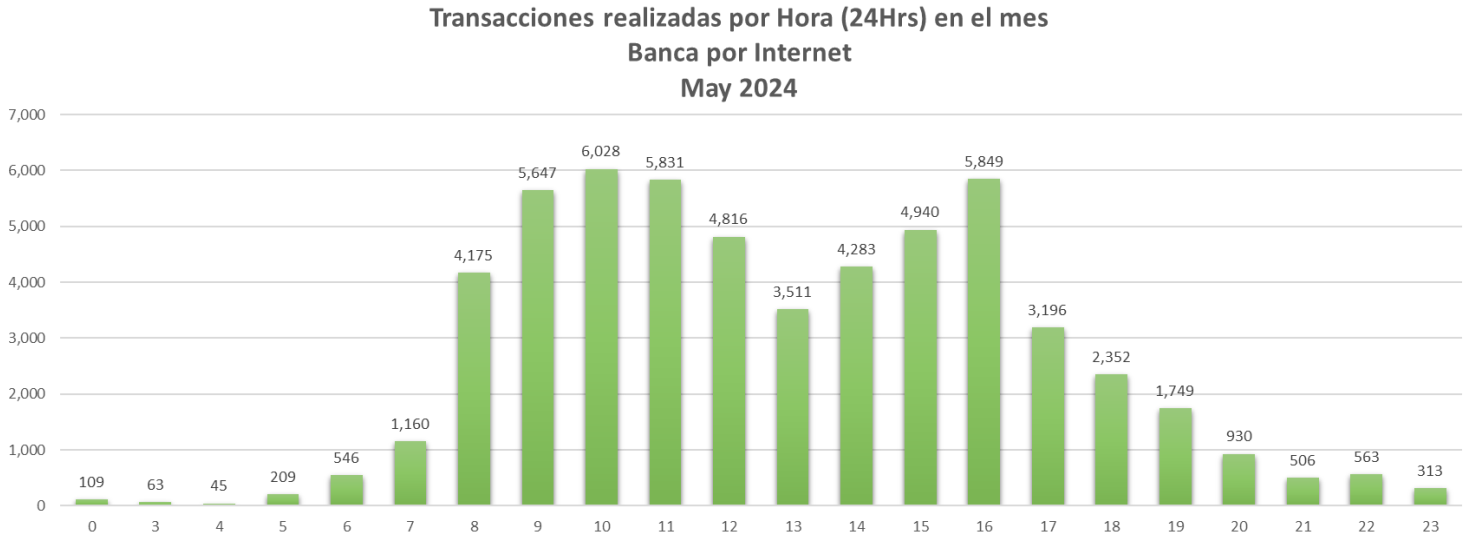
2. Número de Clientes Proyectados para el Proyecto

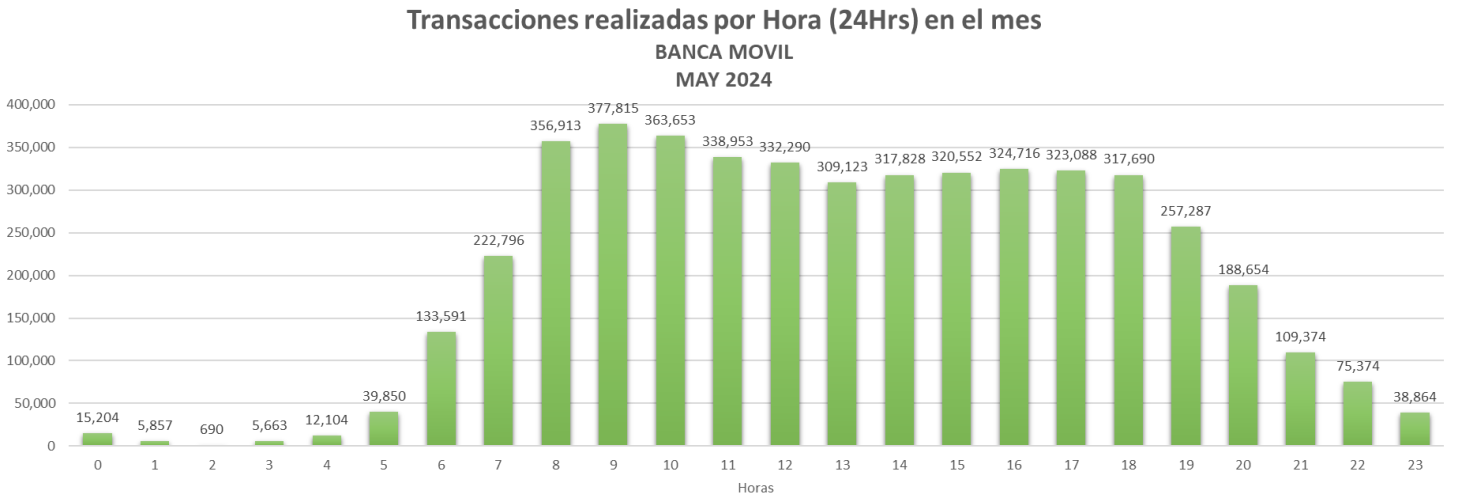
Cantidad total de clientes activos	**5,767,765***

Consumo pico por año al mes	Subtotal financiero y consultas	Financieras y consultas de Cuenta DNI	Total de clientes financieros, consultas y cuenta DNI
Pico máximo mensual 2023	1,770,759	0	**1,770,759**
Pico máximo mensual (Año 1)	1,965,165	411,114	**2,376,279**
Pico máximo mensual incluye cuenta DNI (Año 2)	2,430,330	1,150,000	**3,580,330**
Pico máximo mensual incluye cuenta DNI (Año 3)	2,857,106	2,300,000	**5,157,106**

El pago se realizará de acuerdo con el consumo efectivo mensual y las tarifas por rangos y componentes del servicio que presenten los postores en su oferta económica.
*Fuente: QUIPUS – BN al mes de febrero 2024. Banca Digital – Sección de Canales Alternos (Datos referenciales).

3. Transacciones realizadas por hora (24 horas) por mes





Fuente: Reporte OnDemand TPCT 4050 – Mayo 2024

Anexo N° 6 – Determinación de Rangos por Uso de los Componentes de NUBE

Para completar los datos solicitados en la propuesta, el Contratista debe seguir las siguientes instrucciones:

1. Detallar los rangos de uso para cada componente de la solución, como el almacenamiento en la nube, el procesamiento de datos, la transferencia de datos y otros servicios relevantes.
2. Especificar claramente los límites de uso para cada componente, indicando el volumen máximo de transacciones contemplado en cada rango, para el presente servicio se ha establecido un total de cinco (05) rangos, de menor a mayor, por componente.
3. Proporcionar una descripción de cómo se calcularán y aplicarán los precios por transacción dentro de cada rango de uso.
4. Asegurarse de que los rangos de uso propuestos sean adecuados y estén alineados con las necesidades del proyecto, garantizando la escalabilidad de la solución a lo largo del tiempo.
5. Presentar la información de manera clara y concisa en la propuesta, asegurándose de que sea fácilmente comprensible para el Comité Evaluador.
6. El Contratista podrá añadir más componentes, según su propuesta.

Ítem	Componente	Descripción	Unidad de medida	Rango de uso mensual	Costo Unitarios (S/ Inc. IGV)
1	<Nombre del componente 1>			1 hasta <…>	
				<…> hasta <…>	
				<…> hasta <…>	
				<…> hasta <…>	
				Más de <…>	
2	<Nombre del componente 2>			1 hasta <…>	
				<…> hasta <…>	
				<…> hasta <…>	
				<…> hasta <…>	
				Más de <…>	
3	<Nombre del componente 3>			1 hasta <…>	
				<…> hasta <…>	
				<…> hasta <…>	
				<…> hasta <…>	
				Más de <…>	
4	<Nombre del componente 4>			<Único valor>	
5	<Nombre del componente 5>			<Único valor>	
6	<Nombre del componente 6>			<Único valor>	
7	<Nombre del componente 7>			<Único valor>	

Nota: El pago se realizará de acuerdo con el consumo efectivo mensual y las tarifas por rangos y componentes del servicio que presenten los postores en su oferta económica.

Anexo N° 7 – Índice de Cuadros

Tabla 1: Cuadro de Enrolamiento al Canal Digital ..... - 81 -
Tabla 2: Cuadro de Autenticación del Cliente para la generación de la Clave Dinámica Digital (CDD) ..... - 81 -
Tabla 3: Cuadro de la Arquitectura Tecnológica Referencial de la Banca Móvil y Banca por Internet del Banco de la Nación ..... - 124 -
Tabla 4: Cuadro los Servicios Compartidos ..... - 160 -
Tabla 5: Cuadro del Ambiente de Producción ..... - 161 -
Tabla 6: Cuadro del Ambiente de Certificación (QA) ..... - 163 -
Tabla 7: Cuadro del Ambiente de Desarrollo (DEV) ..... - 165 -
Tabla 8: Cuadro de los Componentes a Demanda ..... - 167 -
Tabla 9:Cruadro de las Especificaciones de Capacidades de los Servicios de Seguridad ..... - 194 -
Tabla 10: Cuadro de Atención de Incidencias del Servicio ..... - 201 -
Tabla 11: Cuadro del Plan de Trabajo ..... - 203 -
Tabla 12: Cronograma de Trabajo para el desarrollo de la Solución ..... - 204 -
Tabla 13: Cuadro de Entregables para los Productos Mínimos Viables (MVP) ..... - 206 -
Tabla 14: Cuadro de la Capacitación Funcional ..... - 209 -
Tabla 15: Cuadro de Aprobación por Área Responsable ..... - 7 -
Tabla 16: Forma de Pago para el Desarrollo e Implementación del Producto. ..... - 8 -
Tabla 17: Forma de pago para los costos fijos el Servicio de Alojamiento, Procesamiento y Seguridad de la Solución ..... - 10 -
Tabla 18: Forma de pago para los costos variables el Servicio de Alojamiento, Procesamiento y Seguridad de la Solución ..... - 12 -
Tabla 19: Cuadro de Requisitos de Calificación ..... - 250 -
Tabla 20: Penalidad por atención de incidencias ..... - 257 -
Tabla 21: Penalidades por Interrupción del Servicio ..... - 258 -

Anexo N° 8 – Índice de Ilustraciones

Ilustración 1: Flujo de activación de una cuenta, enrolamiento al canal digital y activación de CDD (Diagrama referencial) ..... - 51 -
Ilustración 2: Acceso desde la aplicación móvil (imagen referencia) ..... - 52 -
Ilustración 3: Flujo de enrolamiento a la Cuenta DNI ..... - 55 -
Ilustración 4: Flujo de afiliación a la CDD de la Banca Móvil (imagen referencial) ..... - 61 -
Ilustración 5: Mensaje de advertencia para la afiliación de la CDD (imagen referencial) ..... - 63 -
Ilustración 6: Mensaje de confirmación de la activación de la CDD (imagen referencial) ..... - 65 -
Ilustración 7: Constancia de activación notificada el correo electrónico del cliente (imagen referencial) ..... - 65 -
Ilustración 8: Flujo de recuperación de la clave de internet de seis (06) dígitos (Imagen referencial) ..... - 71 -
Ilustración 9: Inicio de sesión de la Banca Móvil propuesto (imagen referencial) ..... - 73 -
Ilustración 10: pantalla de inicio de sesión al Banca por Internet del Banco de la Nación (imagen referencia) ..... - 73 -
Ilustración 11: Mensajes informativos sobre los intentos disponibles para el ingreso de la clave de internet (imagen referencial) ..... - 76 -
Ilustración 12: Pantallas del enrolamiento para la aplicación móvil del Banco de la Nación ..... - 77 -
Ilustración 13: Pantalla de inicio de sesión de la aplicación móvil (imagen referencial) .. - 79 -
Ilustración 14: Máscara informativa de las principales funcionalidades (imagen referencial) ..... - 83 -
Ilustración 15: Pantalla de inicio del Banca por Internet del Banco de la Nación (imagen referencial) ..... - 83 -
Ilustración 16: Movimientos recientes (imagen referencial) ..... - 84 -
Ilustración 17: Accesos directos (imagen referencial) ..... - 85 -
Ilustración 18: Ocultar saldos (imagen referencial) ..... - 85 -
Ilustración 19: Promociones y comunicados (imagen referencial) ..... - 86 -
Ilustración 20: Operaciones favoritas (imagen referencial) ..... - 87 -
Ilustración 21: Menú Anclado (imagen referencial) ..... - 87 -
Ilustración 22: Transferencias bancarias (imagen referencial) ..... - 88 -
Ilustración 23: Transferencia interna (imagen referencial) ..... - 90 -
Ilustración 24: Transferencia interbancaria inmediata (imagen referencial) ..... - 92 -
Ilustración 25: Proceso de transferencia de cuenta interbancaria ..... - 94 -
Ilustración 26: Proceso de transferencia de cuenta a otro Banco ..... - 97 -
Ilustración 27: Ubicación de agencias, cajeros y agentes (imagen referencial) ..... - 115 -
Ilustración 28: Arquitectura híbrida general ..... - 122 -
Ilustración 29: Arquitectura Tecnológica para la Banca Móvil y Banca por Internet del Banco de la Nación (diagrama referencial) ..... - 123 -

Anexo N° 9 – Descripción General de la Metodología para el Ciclo de Vida del Software

La Directiva BN-DIR-8300-147-01 Rev.9 del Ciclo de Vida del Software establecida por el BN, está basada en la Norma Técnica Peruana NTP-ISO/IEC 12207:2016. La citada directiva contiene los principales procesos, actividades, artefactos y buenas prácticas para ser aplicados durante el desarrollo, certificación, operación y mantenimiento de un requerimiento de software aplicativo, el mismo que será entregado al proveedor ganador de la buena pro, luego de firmar el contrato.

La versión detallada de cada proceso, sub-procesos y plantillas de los artefactos se hará entrega al CONTRATISTA en la Fase de Iniciación y Planeamiento del proyecto.

Los procesos principales de la "Metodología para el Ciclo de Vida del Software" son los que a continuación se grafican:

Metodología para el Ciclo de Vida del Software - BN

[1.0] Procesos de Desarrollo de Software:

La Subgerencia Construcción de Aplicaciones es responsable de implementar los procesos principales de desarrollo y mantenimiento que normen el Ciclo de Vida de Software, así como de aplicar el diseño arquitectónico, las metodologías, estándares y/o técnicas que indique la Subgerencia Arquitectura de TIC.

El proceso de Desarrollo contiene actividades de requerimientos de software, diseño, implementación (codificación), integración, pruebas e instalación y aceptación relacionadas con los productos de software, el cual obedece a estándares de diseño de objetos de base de datos, codificación y presentación (pantallas, gráficos, colores, entre otros)..

[2.1] Requerimientos de Software

Es el proceso en el cual se identifican las características o propiedades del producto software, así como también los atributos de calidad y seguridad a satisfacer de los requerimientos funcionales y no funcionales.

[2.2] Diseño del Software

Este proceso da como resultado la definición de la arquitectura, seguridad, componentes, interfaces y otras características de un sistema o componente realizada por la Subgerencia Arquitectura de TIC. El diseño es dividido en dos partes esenciales: El Diseño Arquitectónico y Diseño en detalle de los componentes de la arquitectura.

[2.3] Implementación (codificación segura) y Pruebas del Software

Comprende el desarrollo de cada uno de los componentes del software y los procedimientos de pruebas en el ambiente de desarrollo con el fin de verificar la consistencia de los componentes.

[2.4] Integración

El proceso de Integración permite entregar un conjunto de funciones y capacidades del sistema que pueden ser probadas en su calidad y seguridad antes de su despliegue en el ambiente de certificación.

[2.5] Apoyo a la aceptación del Software

En este proceso se busca demostrar que la implementación de cada requerimiento es adecuada a la necesidad del cliente en el ambiente de desarrollo y por lo tanto aprobada para confirmar que el sistema está listo para su entrega.

[2.6] Transición del Software a Certificación

La transición del software consiste en hacer que el producto desarrollado de software y artefactos relacionados se encuentren disponibles para su despliegue en el ambiente de Certificación y dar inicio a las pruebas con el usuario experto.

[2.0] Procesos de Certificación del Software:

Este proceso permite a la Sección Control de Calidad, verificar y validar la calidad de los productos de software. Esto permite la detección del alineamiento con los estándares definidos. La Certificación de las Pruebas se efectúa a nivel funcional y no funcional de los productos software y consta de los siguientes subprocesos: Planificación, Revisión, Despliegue, Diseño de pruebas, Ejecución de pruebas, Seguimiento y Control, Pase a producción.

[3.0] Procesos de Operación:

En los Procesos de Operación se realiza la instalación y evaluación del software en el entorno del usuario, según las especificaciones establecidas en los manuales de instalación y operación entregadas por el equipo de desarrollo a la Subgerencia de Producción.

[4.0] Proceso de Mantenimiento:

Este proceso se activa cuando el producto de software sufre modificaciones en el código y documentación asociada, debido a un problema o a la necesidad de mejora o adaptación.

Para aquellos proyectos y/o mantenimientos que de manera experimental el Banco utilice marcos de trabajo ágiles, la Directiva del Ciclo de Vida del Software podrá ir incluyendo en forma gradual las mejores prácticas y procesos comprendidos en estas metodologías, con la finalidad de poder complementarla posteriormente.

Entregables determinados para los Proyectos Tercerizados

- Requerimiento de software aprobado
  (Anexo 1 de la Directiva "Gestión de Demanda de TI" BN-DIR-8300-268-01)
- Charter del proyecto
- Solicitud de cambios (si los hubiera)
- Cronograma del proyecto
- Plan de desarrollo de software
- Especificaciones de requerimientos de software
- Especificaciones de casos de uso
- Documento de arquitectura de software
- Documento de especificación detallada de software
- Especificaciones de casos de prueba
- Plan de pruebas
- Resultados de pruebas
- Plan de despliegue
- Acta de certificación
- Manual de usuario
- Manual de operación
- Manual de instalación
- Material de Entrenamiento (diapositivas, tutoriales, demos, guías, etc.)
- Informes de avance (estado)
- Acta de aceptación y Cierre de Proyecto
- Lecciones aprendidas
- Arquitectura de servidores y registro de configuración para gestión de eventos
- Formato de Creación y Mantenimiento de Base de Datos / Tablas
- Formato de Inscripción y/o Mantenimiento de Aplicación
- Formato de Perfiles de Acceso
- Formato para la inscripción en el Sistema de Alertas
- Esquema de Arquitectura de la Solución
- Formato de Control-M
- Formato para Administración de Reportes

Entregables determinados para los Mantenimientos Tercerizados

- Requerimiento de software aprobado
  - (Anexo 2 de la Directiva "Gestión de Demanda de TI" BN-DIR-8300-268-01)
- Solicitud de cambio (si los hubiera)
- Especificaciones de requerimientos de software
- Especificaciones de casos de uso
- Especificaciones de casos de prueba
- Plan de pruebas
- Resultados de pruebas
- Plan de despliegue
- Acta de certificación
- Manual de usuario
- Manual de operación
- Manual de instalación
- Informes de avance (estado)
- Acta de aceptación y cierre
- Lecciones aprendidas
- Formatos de creación de base de datos, inscripción, perfiles, alertas, reportes (de aquellos que hayan sufrido modificaciones)

El CONTRATISTA, deberá realizar estos documentos de acuerdo a los formatos estándar del Banco en cumplimiento de la Metodología del Ciclo de Vida de Software (Ver Anexo 3 de la Directiva BN-DIR-8300-147-01 Rev.9).

Anexo N° 2

Importante

Dependiendo del objeto del contrato, de resultar indispensable, puede incluirse cláusulas adicionales o la adecuación de las propuestas en el presente documento, previo acuerdo de partes.

CONTRATO DE SERVICIO FINANCIERO DE DESARROLLO E IMPLEMENTACIÓN DE LA NUEVA PLATAFORMA DE LOS CANALES DIGITALES (BANCA MOVIL Y BANCA POR INTERNET) DEL BANCO DE LA NACIÓN N°

Conste por el presente documento, el "**Contrato de Servicio Financiero de Desarrollo e Implementación de la nueva plataforma de los canales digitales (Banca Movil y Banca por Internet) del Banco de la Nación**", que celebra de una parte EL BANCO DE LA NACIÓN", en adelante "**EL BANCO**", con RUC Nº 20100030595, con domicilio legal Av. Javier Prado Este N° 2499 – San Borja, representada por [……..…], identificado con DNI Nº [……], y por [……..…], identificado con DNI Nº [……], según poderes inscritos en la Partida Electrónica No. […….] del Registro de Personas Jurídicas de la Zona Registral de Lima y de otra parte […….], con RUC No.[…….], con domicilio en […….], Distrito de [……], Provincia [……] y Departamento de [……], debidamente representado por el […….], identificado(a) con DNI No. […….], según poderes inscritos en la Partida Electrónica No. […….] del Registro de Personas Jurídicas de […..] a quien en adelante se le denominará "**EL CONTRATISTA**".

En adelante, **EL BANCO** y **EL CONTRATISTA** serán denominados de forma conjunta como "**LAS PARTES**", en cuanto corresponda, sin que esto importe un desconocimiento de la calidad de parte que ostentan de manera individual en el presente contrato.

El presente contrato se rige por los Términos de Referencia – TDR que, como **Anexo N°01** forma parte integrante del presente documento, así como las cláusulas contractuales y condiciones siguientes:

CLÁUSULA PRIMERA. - ANTECEDENTES

EL BANCO es una empresa con potestades públicas, integrante del Sector Economía y Finanzas, que opera con autonomía económica, financiera y administrativa, el cual se rige por su Estatuto, aprobado por Decreto Supremo N°07-94-EF, por el Decreto Legislativo N° 1031, Decreto Legislativo que promueve la eficiencia de la actividad empresarial del Estado y su Reglamento, y el artículo 33º de la Ley N° 26702, Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros, y supletoriamente por los demás artículos de dicha Ley General o sus modificatorias.

Asimismo, constituye una de las actividades principales de **EL BANCO**, la realización de operaciones y prestación de servicios para la inclusión financiera y con la finalidad de contribuir al desarrollo económico e inclusión social de acuerdo con las políticas nacionales que se emitan para tal fin.

Por su parte, **EL CONTRATISTA** es una empresa constituida como [……], cuyo objetivo social es la [……...…… … ……..], como los requeridos por **EL BANCO**.

De conformidad con lo establecido en el artículo 4° literal a) de la Ley N°30225 – Ley de Contrataciones del Estado, con lo señalado por la Ley General del Sistema Financiero y del

Sistema de Seguros y Orgánica de la Superintendencia de Banca, Seguros y AFP — Ley N° 26702 sobre el término "servicio financiero" incluido en el Anexo - Glosario y con los literales h), o) y p) del artículo 12.20 del Capítulo 12 del Acuerdo Comercial con los Estados Unidos (TLC), el presente es un contrato de naturaleza bancaria y/o financiera, por lo que se encuentra fuera del ámbito de aplicación de la normativa de Contrataciones del Estado.

CLÁUSULA SEGUNDA: OBJETO DEL CONTRATO

Por medio del presente contrato, en adelante, **EL CONTRATO**, **EL BANCO** contrata los servicios de **EL CONTRATISTA** con el objeto del desarrollo e implementación de la nueva plataforma de los canales digitales Banca Móvil y Banca por Internet del Banco de la Nación. Así como el desarrollo de las interfaces de programación de aplicaciones (APIs) necesarios para su implementación, en adelante el **SERVICIO**.

El **SERVICIO** será prestado por **EL CONTRATISTA** a **EL BANCO**, de conformidad con el alcance y descripción del **SERVICIO** que se encuentra descrito en el numeral 7 del **Anexo N°01**, el cual está compuesto por los siguientes Ítems, lo cual **EL CONTRATISTA** deberá cumplir en su integridad:

- Descripción y Condiciones del Servicio
- Enrolamiento al Canal Digital
- Enrolamiento a la Cuenta DNI
- Afiliación a la Clave Dinámica Digital (CDD)
- Gestión de Claves Centralizadas
- Recuperación de la clave de Internet
- Primer Inicio de Sesión
- Inicio de Sesión del Cliente Recurrente
- Factores de Autenticación y Seguridad del Cliente
- Consulta de Productos, Saldos y Movimientos
- Transferencias Bancarias
- Retiro sin Tarjeta y por Agentes Corresponsales
- Módulo de Seguridad
- Configuración de Multidioma
- Pago de Servicios y pago a Empresas
- Recargas Móviles
- Actualización de Datos Personales
- Operaciones Favoritas
- Giros Nacionales
- Bloqueo de Tarjeta de Débito o Crédito
- Pago de Tarjetas de Crédito
- Créditos Digitales y Seguros
- Consulta de Estado de Cuenta
- Configuración de los Atributos de Cuentas y Tarjetas del cliente
- Módulo de Administración (backoffice)
- Pago de Tasas
- Cuenta DNI

CLÁUSULA TERCERA: MONTO CONTRACTUAL

EL BANCO pagará por la prestación del **SERVICIO**, la suma total de […….....] con ../100 Soles (S/ ……..), que incluye todos los impuestos de Ley, conforme a la forma de pago señalado en la Propuesta Comercial que forma parte integrante del presente **CONTRATO** como **Anexo N° 2.**

Este monto comprende el costo del **SERVICIO**, todos los tributos, seguros, transporte, inspecciones, pruebas y, de ser el caso, los costos laborales conforme la legislación vigente, así como cualquier otro concepto que pueda tener incidencia sobre la ejecución del **SERVICIO** materia del presente **CONTRATO**. De igual manera, el costo incluye el desarrollo e implementación de las APIs por parte de **EL CONTRATISTA**, los mismos que son necesarios para el **SERVICIO**. En ese sentido, en ningún supuesto, tales costos estarán sujetos a pagos adicionales o diferenciados al costo total del **SERVICIO**.

CLÁUSULA CUARTA: DEL LUGAR Y PRESTACIÓN DEL SERVICIO, DEL PAGO Y DE LA GARANTÍA

La prestación del **SERVICIO** se realizará en la sede principal de **EL BANCO**, ubicada en Av. Javier Prado Este 2499 – San Borja, según lo establecido en el numeral 19 del **Anexo N°01**. El desarrollo del proyecto podrá ser realizado de forma remota. No obstante, **EL BANCO** tendrá la opción de solicitar presencialidad en caso lo considere necesario. Las actividades y las reuniones de trabajo con el personal del Banco se llevarán a cabo a través de la Plataforma Virtual del Banco o en la mencionada oficina principal.

EL BANCO se obliga a pagar la contraprestación del **SERVICIO** al Contratista en moneda Soles (S/) y de acuerdo al siguiente detalle:

4.1. Por el servicio de diseño, desarrollo e implementación de la solución, se realizará en diez (10) armadas condicionadas a la emisión del Acta de Conformidad correspondiente al cumplimiento de los entregables definidos, así como al cumplimiento de sus especificaciones y conforme el procedimiento de aprobación señalados en los numerales 15 y 16 del **Anexo N°01**, según los plazos para el cumplimiento de los entregables y porcentajes de pago siguientes:

N°	Entregable	Referencia establecida en el Anexo N° 01 (Términos de Referencia – TDR)	Días calendarios del plazo de entregables, contados desde la aprobación del Plan de Trabajo	Porcentaje de Facturación por desarrollo de Solución
1	Análisis funcional	7. ALCANCE Y DESCRIPCIÓN DEL SERVICIO	60	5.00%
2	Diseño UX / UI	7. ALCANCE Y DESCRIPCIÓN DEL SERVICIO 7.1. Descripción y condiciones del servicio, literal "c".	75	5.00%
3	Codificación y Pentesting MVP 1	7.2. Enrolamiento al canal digital 7.3. Enrolamiento a la Cuenta DNI 7.4 Afiliación a la Clave Dinámica Digital (CDD) 7.5 Gestión de Claves Centralizadas 7.6 Recuperación de la contraseña de Internet 7.7 Primer Inicio de Sesión 7.8 Inicio de Sesión del Cliente Recurrente 7.9 Factores de Autenticación y Seguridad del Cliente 7.10 Consultas de Productos, Saldos y Movimientos 7.11 Transferencias Bancarias 7.12 Retiro sin tarjeta y por agentes corresponsales 7.13 Módulo de Seguridad 7.14 Configuración de Multidioma (lenguas originarias)	165	11.00%

4	Despliegue en Producción MVP 1	-	180	14.50%
5	Codificación y Pentesting MVP 2	7.15 Pago de Servicios y pago a empresas 7.16 Recargas móviles 7.11 Transferencias Bancarias (Diferidas) 7.17 Actualización de Datos Personales 7.18 Operaciones Favoritas 7.19 Giros Nacionales 7.20 Bloqueo de Tarjetas de Débito o de Crédito	255	9.00%
6	Despliegue en Producción MVP 2	-	270	13.50%
7	Codificación y Pentesting MVP 3	7.21 Pago de Tarjeta de Crédito 7.22 Créditos Digitales 7.23 Consulta de Estado de Cuenta 7.24 Ubicación de Agencias, Cajeros y Agentes 7.25 Configuración de los atributos de Cuentas y Tarjetas de los clientes	345	9.00%
8	Despliegue en Producción MVP 3	-	360	13.50%
9	Codificación y Pentesting MVP 4	7.26 Módulo de Administración 7.27 Pago de Tasas	405	9.00%
10	Despliegue en Producción MVP 4	-	420	10.50%
			Total	**100.00%**

Para efectos del pago de las contraprestaciones ejecutadas, **EL CONTRATISTA** deberá remitir a **EL BANCO** la documentación siguiente:

a) Carta simple dirigida a la Subgerente de Compras de la Gerencia de Administración y Logística de **EL BANCO**;
b) Factura o comprobante de pago;
c) Acta de conformidad original de la Subgerencia de Innovación Digital de **EL BANCO**;
d) Informe de la Subgerencia de Innovación Digital y anexos, de corresponder.

La presente documentación se debe presentar en formato físico en el Módulo de Mesa de Partes de la Sede Central del Banco de la Nación, sito en Calle Arqueología N°120 - San Borja, en horario de oficina.

4.2. Por los servicios de alojamiento, procesamiento y seguridad de la solución, los pagos se efectuarán por prestaciones completadas de acuerdo a las tarifas establecidas para cada rango, modalidad de validación y los consumos mensuales de prestaciones efectivas y debidamente acreditadas, según los requisitos solicitados y la propuesta comercial establecida en el **Anexo N° 02**.

4.2.1. **Forma y plazo para el pago del servicio de alojamiento procesamiento y seguridad. -** Los pagos se realizarán en base a la implementación de los hitos propuestos, según los plazos para el cumplimiento de los entregables y porcentajes de pago siguientes:

Implementación del servicio de nube	Hitos	Referencia establecida en el Anexo N° 01 (Términos de Referencia – TDR)	Plazo máximo de entrega (en días calendarios)	Porcentaje (%) de pago
Para el pago de la implementación de la infraestructura	Despliegue Base para los Ambientes	21.2 Servicios de Alojamiento, Procesamiento y Seguridad de la Solución, literal b.1 Para el Pago de la Implementación de la Infraestructura, literal b.1.1 Despliegue Base para los Ambientes	55 días posteriores a la fecha de la firma del acta de conformidad del plan de trabajo.	25% del costo de implementación de la infraestructura
	Despliegue del Ambiente de Desarrollo (DEV)	21.2 Servicios de Alojamiento, Procesamiento y Seguridad de la Solución, literal b.1 Para el Pago de la Implementación de la Infraestructura, b.1.2 Despliegue del Ambiente de Desarrollo (DEV)	35 días posteriores a la fecha de aprobación del informe técnico de Despliegue base para los ambientes.	25% del costo de implementación de la infraestructura
	Despliegue del Ambiente de Calidad (QA)	21.2 Servicios de Alojamiento, Procesamiento y Seguridad de la Solución, literal b.1 Para el Pago de la Implementación de la Infraestructura, b.1.3 Despliegue del Ambiente de Calidad (QA)	35 días posteriores a la fecha de aprobación del informe técnico de Despliegue del ambiente de desarrollo.	25% del costo de implementación de la infraestructura
	Despliegue del Ambiente de Producción (PRD)	21.2 Servicios de Alojamiento, Procesamiento y Seguridad de la Solución, literal b.1 Para el Pago de la Implementación de la Infraestructura, b.1.4 Despliegue del Ambiente de Producción (PRD)	35 días posteriores a la fecha de aprobación del informe técnico de Despliegue del ambiente de calidad.	25% del costo de implementación de la infraestructura
Para el pago de la implementación del ambiente de seguridad	Servicio de Implementación Plataforma de Protección para Aplicaciones CNAPP	21.2 Servicios de Alojamiento, Procesamiento y Seguridad de la Solución, literal b.2 Para el Pago de la Implementación del Ambiente de Seguridad, b.2.1 Servicio de Implementación Plataforma de Protección para Aplicaciones CNAPP	60 días posteriores a la fecha del informe de aprobación del ambiente de desarrollo (DEV).	25% del costo de implementación del ambiente de seguridad

	Servicio Implementación Firewall	21.2 Servicios de Alojamiento, Procesamiento y Seguridad de la Solución, literal b.2 Para el Pago de la Implementación del Ambiente de Seguridad, b.2.2 Servicio Implementación Firewall		25% del costo de implementación del ambiente de seguridad
	Servicio Implementación SaaS de Seguridad para los servicios WAF, ataques volumétricos de denegación de servicio y servicio de seguridad de API Discovery	21.2 Servicios de Alojamiento, Procesamiento y Seguridad de la Solución, literal b.2 Para el Pago de la Implementación del Ambiente de Seguridad, b.2.3 Servicio Implementación SaaS de Seguridad para los Servicios WAF, Ataques Volumétricos de Denegación de Servicio y Servicio de Seguridad de API Discovery		25% del costo de implementación del ambiente de seguridad
	Servicio Implementación para el Servicio de Detección Avanzada para ataques de Bots Automatizados	21.2 Servicios de Alojamiento, Procesamiento y Seguridad de la Solución, literal b.2 Para el Pago de la Implementación del Ambiente de Seguridad, b.2.4 Servicio Implementación para el Servicio de Detección Avanzada para Ataques de Bots Automatizados		25% del costo de implementación del ambiente de seguridad

Implementación del servicio de nube	**Hitos**	**Referencia establecida en el Anexo N° 01 (Términos de Referencia – TDR)**	**Plazo máximo de entrega (en días calendarios)**
Para el pago mensual por uso de infraestructura y ambiente de seguridad	Pago mensual de infraestructura	21.2 Servicios de Alojamiento, Procesamiento y Seguridad de la Solución, literal b.3 Para el Pago Mensual por Uso de Infraestructura y Ambiente de Seguridad, b.3.1 Pago Mensual de Infraestructura	El pago por el uso de los componentes de infraestructura se realizará al final de cada mes según los consumos realizados por cada uno de estos componentes especificados en las Tablas de Capacidades. (considerar DEV, QA, PRD, seguridad y compartidos).
	Pago mensual del servicio de seguridad	21.2 Servicios de Alojamiento, Procesamiento y Seguridad de la Solución, literal b.3 Para el Pago Mensual por Uso de Infraestructura y	

		Ambiente de Seguridad, b.3.2 Pago Mensual del Servicio de Seguridad	
Para el pago del soporte técnico	Pago mensual por soporte técnico	21.2 Servicios de Alojamiento, Procesamiento y Seguridad de la Solución, literal b.4 Para el Pago del Soporte Técnico, b.4.1 Pago Mensual de Soporte Técnico	El pago por el soporte y mantenimiento de la infraestructura y seguridad se realizará al final de cada mes, hasta el final del contrato, iniciándose este soporte y mantenimiento al finalizar la implementación del ambiente de producción

Las especificaciones para el pago de la Implementación de la Infraestructura (b.1), Implementación del Ambiente de Seguridad (b.2), Pago Mensual por Uso de infraestructura y Ambiente de Seguridad (b.3) y Pago del Soporte Técnico (b.4) se encuentran establecidas en el numeral 21.2 del **Anexo N° 01.**

De igual manera, la documentación para los pagos se deberá presentar en formato físico en el Módulo de Mesa de Partes de la Sede Central del Banco de la Nación, sito en Calle Arqueología N°120 - San Borja, en horario de oficina, de acuerdo con

4.3. Por el servicio de Integración de la CUENTA DNI (Componente opcional), se realizará de acuerdo a las especificaciones precisadas en el numeral 7.28 del **Anexo N° 01.** El pago se efectuará contra el Acta de Conformidad del diseño, desarrollo e implementación del servicio de integración de la Cuenta DNI, emitido por la Subgerencia Innovación Digital de la Gerencia de Banca Digital. Además del informe técnico favorable de la validación por parte de la Gerencia de Tecnología de la Información.

4.4. Por el servicio de Asistencia para Alcanzar la Mejora Continua de la Solución, se realizará de acuerdo a las especificaciones precisadas en los numerales 7 y 33 del **Anexo N° 01**. El pago se llevará a cabo mensualmente, o según lo acordado con **EL BANCO**, una vez se haya recibido y aprobado el Acta de Conformidad correspondiente. Este pago se realizará conforme al sistema de precio unitario y basado en el consumo de horas utilizadas durante el periodo facturado, de acuerdo con el Anexo N° 02 (Propuesta Comercial).

4.5. EL BANCO pagará dentro de los quince (15) días calendario siguientes a la conformidad de cada entregable de **EL SERVICIO**, siempre que se verifiquen las condiciones y especificaciones establecidas en la presente cláusula y en el **Anexo N° 01**. En caso de discrepancias entre el presente **CONTRATO** y el **Anexo N°01** prevalecerán las disposiciones contenidas en este último por tratarse de los Términos de Referencia – TDR que contienen las especificaciones de **EL SERVICIO**.

De la Garantía

A la firma del presente **CONTRATO, EL CONTRATISTA** entrega una Carta Fianza incondicional, solidaria, irrevocable y de realización automática a solo requerimiento de **EL BANCO.** Esta garantía deberá ser emitida por una empresa que se encuentre bajo la supervisión directa de la Superintendencia de Banca, Seguros y Administradoras Privadas de Fondo de Pensiones y que cuenten con clasificación de riesgo B o superior. Asimismo, deben estar autorizadas para emitir garantías; o estar consideradas en la última lista de Bancos extranjeros de primera categoría que periódicamente publica el Banco Central de Reserva del Perú.

La Carta Fianza deberá ser emitida a favor de EL BANCO por una suma equivalente al diez por ciento (10%) del monto total del **CONTRATO**, la misma que debe mantenerse vigente hasta la conformidad de la recepción del **SERVICIO**.

CLÁUSULA QUINTA: VIGENCIA DEL CONTRATO

Prestación Principal:
El plazo de la prestación del servicio de diseño, desarrollo e implementación de la nueva plataforma bancaria para los canales digitales Banca Móvil y Banca por Internet de **EL BANCO** será de 420 (cuatrocientos veinte) días calendario computados desde el día siguiente de la aprobación del Plan de Trabajo hasta la conformidad de la recepción del **SERVICIO**.

Prestaciones Accesorias:
El plazo de la prestación de los servicios de alojamiento, procesamiento y seguridad de la solución (servicio de nube) será de 36 (treinta y seis) meses computados desde el día siguiente de la aprobación del Plan de Trabajo.

El plazo de la prestación de los servicios de integración de la Cuenta DNI será de 150 (ciento cincuenta) días computados desde la fecha de confirmación sobre el inicio de la ejecución de la presente prestación por parte de **EL BANCO**.

El plazo de la prestación de los servicios de asistencia para alcanzar la Mejora Continua de la Solución tendrá una duración de 90 (noventa) días calendarios computado desde el día siguiente de la suscripción del Acta de Conformidad correspondiente al MVP 4, bajo la modalidad de bolsa de trabajo que considera 600 (seiscientas) horas mensuales y un total de 1,800 (mil ochocientas) horas. Terminado el periodo de 90 (noventa) días, la modalidad del servicio será a demanda durante el tiempo de ejecución del **CONTRATO.**

CLÁUSULA SEXTA. - OBLIGACIONES DE EL CONTRATISTA

EL CONTRATISTA se compromete a cumplir con las obligaciones, responsabilidades y condiciones del **SERVICIO** contratado, de acuerdo con las reglas de la buena fe y común intención de **LAS PARTES**, conduciéndose con honestidad y responsabilidad; y de manera general a cumplir con las siguientes obligaciones:

6.1. Realizar todos los trabajos y/o actividades conforme a lo dispuesto en **EL CONTRATO**, así como en los **Anexos Nos. 01** y **02** que forman parte del mismo; las normativas y lineamientos de **EL BANCO** lo cual implica prestar **EL SERVICIO** siempre en función de la protección de los intereses de **EL BANCO**.

6.2. Cumplir oportunamente con los entregables de cada **SERVICIO** y en los plazos establecidos en el **Anexo N°01** del presente **CONTRATO.**

6.3. Permitir a **EL BANCO** realizar la supervisión de la ejecución del **SERVICIO,** de acuerdo al Cronograma de Trabajo para el desarrollo de la solución.

6.4. La emisión de conformidad de los documentos que conforman el producto final no convalida los defectos o vicios ocultos de la solución que no sean posibles advertir al momento de su revisión y/o certificación por parte de **EL BANCO**, por lo que **EL CONTRATISTA** se compromete a subsanarlas incluido durante el periodo de garantía, sin perjuicio del derecho de **EL BANCO** de reclamar los daños y perjuicios, en caso **EL CONTRATISTA** no subsane y/o repare.

6.5. Abstenerse de realizar acciones u omisiones que perjudiquen la imagen institucional de **EL BANCO,** manteniendo la confidencialidad de la información proporcionada por **EL BANCO** para la prestación del servicio, sin divulgar, revelar, entregar o poner a disposición de terceros, ya sea en o fuera del lugar de trabajo, a menos que cuente con una autorización expresa de **EL BANCO,** de acuerdo a lo establecido en la cláusula décima cuarta de **EL CONTRATO**.

6.6. Para el desarrollo de la prestación de **EL SERVICIO**, deberá contar en todo momento con los recursos de personal calificado que deberá cumplir con las cualidades profesionales y experiencia señalada en el **Anexo N°01** de **EL CONTRATO**. Asimismo, **EL CONTRATISTA** se obliga a informar por escrito a **EL BANCO** la relación del personal que accederá a sus instalaciones, la misma que mantendrá actualizada cada tres (03) meses, y en su caso informar a **EL BANCO** con dos (02) días de anticipación como mínimo, el cambio de cualquiera de su personal a través del cual presta **EL SERVICIO**. El acceso del personal de **EL CONTRATISTA** a las instalaciones de **EL BANCO** requerirá la autorización previa de este último.

6.7. Para los casos de contratación de desarrollo de software a medida, **EL CONTRATISTA** se compromete a elaborar los documentos relacionados con sus entregables, de acuerdo con los formatos estándares de **EL BANCO** en cumplimiento a la Metodología de Ciclo de Vida de Software que le ha sido proporcionado por **EL BANCO** como parte del **Anexo N°01** de **EL CONTRATO**.

EL CONTRATISTA se compromete, sin generar costo adicional para **EL BANCO**, a la implementación de todos los aspectos funcionales que este requiera y que se encuentren en el alcance de su propuesta comercial.

6.8. Implementar las medidas de seguridad necesarias para garantizar la ejecución de **EL SERVICIO,** así como la integridad de la documentación y los entregables de **EL SERVICIO** proporcionados por **EL CONTRATISTA**.

6.9. Verificar que las herramientas tecnológicas, los programas del sistema y, en general, toda implementación realizada por **EL CONTRATISTA** sobre **EL SERVICIO** contratado, cumplan con las condiciones, especificaciones técnicas y requisitos señalados en el **Anexo N°01.**

6.10. Brindar la información y/o documentación solicitada por **EL BANCO** relacionadas a las obligaciones contraídas en el presente **CONTRATO**, así como cualquiera necesaria para cumplir con las disposiciones normativas y regulatorias que regulan las actuaciones de **EL BANCO**.

6.11. Mantener vigente la Carta Fianza de fiel cumplimiento durante la vigencia del **CONTRATO** hasta la conformidad de la recepción del **SERVICIO**.

6.12. Reembolsar íntegramente las costas, costos y cualquier importe que tenga que pagar a **EL BANCO** para hacer frente a acciones judiciales, extrajudiciales o administrativas iniciadas en su contra, como consecuencia del incumplimiento de las obligaciones o la deficiente prestación del servicio por parte de **EL CONTRATISTA**, siempre que este no se haya originado por un hecho fortuito o fuerza mayor o a cualquier causa imputable debidamente comprobada a **EL BANCO**.

Esta obligación se extiende a las indemnizaciones, multas o cualquier pago que **EL BANCO** sea requerido a pagar, ya sea por una autoridad judicial o administrativa, por resolución o sentencia en última instancia, por haber sido declarado responsable solidario de **EL CONTRATISTA**, que se originen en el incumplimiento de las obligaciones por causa imputable a **EL CONTRATISTA**.

6.13. Se compromete a no subcontratar el servicio o alguna de las actividades contempladas en **EL CONTRATO**, sin previa autorización y por escrito de **EL BANCO**, así como tampoco ceder su posición contractual, salvo autorización expresa de **EL BANCO**.

6.14. A la suscripción del contrato deberá presentar obligatoriamente una declaración jurada que cumple las disposiciones establecidas en la Ley N° 29783 - Ley de Seguridad y Salud

en el Trabajo y su Reglamento, así como la Declaración Jurada de no encontrarse inscrito en el Registro de Deudores de Reparación Civil.

CLÁUSULA SEPTIMA. - OBLIGACIONES DE EL BANCO

7.1. Proporcionar desde el inicio de **EL CONTRATO** la infraestructura (hardware, software base, equipos HSM, equipos de seguridad, comunicaciones u otros) y requerimientos (información, recursos, facilidades y otros) solicitados por **EL CONTRATISTA**, de ser el caso y según corresponda al **SERVICIO** contratado, así como el cumplimiento de las actividades de responsabilidad de **EL BANCO** o terceros, que fuesen necesarios para el cumplimiento de las obligaciones de **EL CONTRATISTA,** según lo descrito en el **Anexo N° 01** de **EL CONTRATO.**

7.2. Realizar los ajustes y cambios necesarios del lado de las aplicaciones internas (canales, sistema host, sistema de control de accesos -ISIM u otros) o de terceros para su integración y funcionamiento con la solución provista en el **SERVICIO.**

7.3. **EL BANCO** estará a cargo de brindar la conformidad en sus ambientes de pruebas y su correcta configuración con el software base, con la finalidad de verificar que se coloque en producción con la participación y soporte técnico especializado de **EL CONTRATISTA**.

7.4. Las demás obligaciones señaladas en el presente **CONTRATO.**

CLÁUSULA OCTAVA. – DE LA GARANTÍA

EL CONTRATISTA asumirá la responsabilidad por la calidad de la solución provista, por lo que, de presentarse fallas de diseño o técnico sobre el desarrollo del software, así como respecto a la disponibilidad o funcionamiento de los componentes alojados en la nube y, en general, cualquier supuesto que resulte ajeno al uso normal, habitual y correcto de los servicios que no fueron detectados al momento del otorgamiento de la conformidad por parte de **EL BANCO**, **EL CONTRATISTA** deberá realizar las correcciones necesarias para subsanar las observaciones planteadas y debidamente sustentadas por **EL BANCO** dentro del plazo no mayor de quince (15) días calendario, dependiendo de la complejidad de las mismas podrá solicitar la ampliación de un plazo adicional. Se deja constancia que estas correcciones serán realizadas sin costo alguno para **EL BANCO** durante el periodo de garantía.

Asimismo, **EL CONTRATISTA** como responsable de la solución provista a **EL BANCO**, deberá garantizar la calidad de los servicios realizados, de acuerdo con las normas legales, durante el periodo de la garantía, por lo que, en caso de ser requerido para cualquier aclaración o corrección, deberá concurrir y atender los requerimientos que **EL BANCO** hubiere solicitado.

LAS PARTES acuerdan que el periodo de garantía del **SERVICIO** se iniciará después de poner en producción el último entregable que corresponde al MVP 4, y **EL CONTRATISTA** garantizará el correcto funcionamiento por un periodo mínimo de un (01) año.

CLÁUSULA NOVENA.- PENALIDADES

Si **EL CONTRATISTA** incurre en retraso injustificado en la ejecución de las prestaciones objeto del contrato, **EL BANCO** le aplica automáticamente una penalidad por mora por cada día de atraso sobre el monto total del respectivo entregable, de acuerdo a la siguiente fórmula:

$$\text{Penalidad Diaria} = \frac{0.10 \times \text{monto vigente de la fase}}{F \times \text{plazo vigente en días}}$$

Donde:
F = 0.25

Se considera justificado el retraso y en consecuencia no se aplica penalidad, cuando **EL**

CONTRATISTA acredite, de modo objetivamente sustentado, que el mayor tiempo transcurrido no le resulta imputable; acreditación que deberá contar con el asentimiento por escrito de **EL BANCO**, según sus procedimientos internos.

Otras Penalidades Aplicables
Se establece las siguientes penalidades aplicables al contratista ante el incumplimiento injustificado de sus obligaciones contractuales:

- **Penalidad 1.- Por sustitución del personal profesional**

Nº	PENALIDAD	MONTO DE LA PENALIDAD	VERIFICACIÓN Y PROCEDIMIENTO DE APLICACIÓN DE LA PENALIDAD
1	Cualquier cambio deberá ser comunicado al Banco, si el Contratista cambia alguno(s) de los profesionales del personal propuesto sin autorización del Banco de la Nación se le aplicará una penalidad de una (01) UIT; la cual será deducida en el periodo de pagos en que se haya observado el incumplimiento.[21]	1 UIT	Informe (o Acta) de [.....]

- **Penalidad 2.- Por atención de incidencias**

Penalidades por atención de incidencias			
N°	**Supuestos de aplicación de Penalidad**	**Forma de Cálculo**	**Procedimiento**
1. Atención de Incidentes por nivel			
1.1	**Crítica**	La atención supera 30 minutos, se le aplicara 0.5 de una UIT	Informe de la Subgerencia de Producción sobre el incumplimiento del horario de atención
1.2	**Alta**	La atención supera 1 hora, se le aplicara 0.4 de una UIT	
1.3	**Media**	La atención supera 2 horas, se le aplicara 0.3 de una UIT	
1.4	**Baja**	La atención supera 4 horas, se le aplicara 0.2 de una UIT	
2. Solución del incidente por nivel			
2.1	**Crítica**	La atención supera 1 hora, se le aplicara 0.5 de una UIT	Informe de la subgerencia de producción o de la Oficina de Seguridad informática sobre el incumplimiento del tiempo de solución
2.2	**Alta**	La atención supera 2 horas, se le aplicara 0.4 de una UIT	
2.3	**Media**	La atención supera 4 horas, se le aplicara 0.3 de una UIT	
2.4	**Baja**	La atención supera 24 horas, se le aplicara 0.2 de una UIT	
3. Entrega de Informe de Remediación por nivel de incidente			
3.1	**Crítico**	La atención supera 10 días, se le aplicara 0.5 de una UIT	Informe de la subgerencia de producción o la Oficina de Seguridad Informática sobre el incumplimiento del tiempo de entrega de
3.2	**Alta**	La atención supera 12 días, se le aplicara 0.4 de una UIT	
3.3	**Media**	La atención supera 14 días,	

[21] Pliego de Consultas N° 01-2024 - Concurso de Méritos (Consulta N° 53 TCO LATAM).

		se le aplicara 0.3 de una UIT	informe de remediación.
3.4	**Baja**	La atención supera 16 días, se le aplicara 0.2 de una UIT	

- **Penalidad 3.- Por Interrupción del Servicio.**

Descripción	Penalidad	Base de Cálculo	Procedimiento
Interrupción del servicio de nube por cada 5 minutos acumulados en el mes	0.5	UIT	La Subgerencia de Producción informará las ocurrencias de manera mensual sobre los minutos de servicio de nube interrumpidos mensualmente y el monto será ejecutado de la facturación mensual del servicio de infraestructura.
Interrupción del servicio de seguridad cada 5 minutos acumulados en el mes	0.5	UIT	La Subgerencia de Producción informará las ocurrencias de manera mensual sobre los minutos de servicio de seguridad interrumpidos mensualmente y el monto será ejecutado de la facturación mensual del servicio de seguridad.
Interrupción del servicio de aplicaciones cada 5 minutos acumulados en el mes	0.5	UIT	La Subgerencia de Producción informará las ocurrencias de manera mensual sobre los minutos de servicio de aplicaciones interrumpidos mensualmente y el monto será ejecutado de la facturación mensual del servicio de soporte y mantenimiento. Esta penalidad no aplicará si verifica que existe una falla en el servicio de nube como origen del incidente.

Estas penalidades se deducen de los pagos a cuenta o del pago final, según corresponda; o, si fuera necesario, se cobrará del monto resultante de la ejecución de la garantía de fiel cumplimiento.

La penalidad por mora y otras penalidades pueden alcanzar cada una un monto máximo equivalente al diez por ciento (10%) del monto del contrato vigente. Cuando se llegue a cubrir el monto máximo de la penalidad por mora o el monto máximo para otras penalidades, **EL BANCO** puede resolver el contrato por incumplimiento de pleno derecho, conforme a lo dispuesto por el artículo 1430° del Código Civil.

CLÁUSULA DÉCIMA. - RESOLUCIÓN DEL CONTRATO

LAS PARTES declaran que podrá resolverse **EL CONTRATO**, por cualquiera de los siguientes supuestos:

10.1. **EL CONTRATISTA** o **EL BANCO** incumpla con alguna de las obligaciones establecidas en el presente **CONTRATO,** con excepción de las señaladas en las cláusulas décima segunda, décima cuarta, décima sexta, décima séptima y décima octava, la parte que se ve afectada con el incumplimiento procederá a requerir a su contraparte, mediante carta vía notarial, que cumpla con su obligación dentro de un plazo no menor de quince (15) días hábiles bajo apercibimiento de resolver **EL CONTRATO**. Si la obligación no se cumple dentro del plazo señalado, **EL CONTRATO** se resolverá de pleno derecho, sin perjuicio del pago de la indemnización por daños y perjuicios correspondientes, en atención a lo dispuesto por el artículo 1429° del Código Civil.

10.2. **EL CONTRATISTA** incumpla con las obligaciones precisadas en las cláusulas décima segunda, décima cuarta, décima sexta, décima séptima y décima octava del presente **CONTRATO**, en aplicación de lo establecido en el artículo 1430° del Código Civil**.**

10.3. Por mutuo acuerdo de **LAS PARTES**, el que deberá constar por escrito.

10.4. Por caso fortuito o fuerza mayor debidamente comprobado, que imposibilite el cumplimiento de las obligaciones contraídas en el presente Contrato.

LAS PARTES acuerdan expresamente que el término de EL CONTRATO no afectará la culminación de las obligaciones **pendientes** a la fecha de su resolución, salvo cuando esta se haya producido por caso fortuito o fuerza mayor, o debido a la causal de incumplimiento que no permita a la otra parte continuar con las actividades asumidas, a menos que LAS PARTES convengan lo contrario.

CLÁUSULA DÉCIMA PRIMERA. – **DE LA PROPIEDAD INTELECTUAL**

LAS PARTES acuerdan que **EL CONTRATISTA** cede de manera ilimitada, exclusiva y gratuita los derechos patrimoniales de propiedad intelectual y formas de explotación sobre los diseños, invenciones, prototipos, informes, manuales, protocolos, datos, documentación, entregables y demás categorías, así como de todos los activos intangibles (data, *know-how* e información protegida como secreto empresarial) que se generen en el **SERVICIO** contratado, a favor de **EL BANCO.**

Además, **EL CONTRATISTA** cede a favor de **EL BANCO**, de forma exclusiva y sin restricciones, los derechos sobre los recursos siguientes:

- **Códigos fuente:** Todos los códigos fuente desarrollados para la implementación de la nueva plataforma bancaria, incluyendo aplicaciones móviles, web y backend. Asimismo, **EL CONTRATISTA** deberá hacer entrega de los formatos o archivos editables utilizados en la etapa de análisis y diseño UX/UI.
- **Librerías de software:** Todas las librerías de software de terceros utilizadas en el desarrollo de la plataforma, junto con las licencias correspondientes que permitan su uso y modificación por parte de **EL BANCO**.
- **Documentación técnica:** Documentación completa y actualizada de la plataforma. **EL CONTRATISTA** deberá elaborar estos documentos de acuerdo con los formatos estándares de **EL BANCO** en cumplimiento de la Metodología del Ciclo de Vida de Software señalado en el **Anexo N°01**. En caso de que **EL BANCO** y **EL CONTRATISTA** acuerden la no aplicabilidad de un documento específico, **EL CONTRATISTA** deberá formalizar dicha decisión mediante un correo electrónico que detalle los motivos de la misma, el mismo que deberá ser aprobado por **EL BANCO**.
- **Otros recursos:** Cualquier otro recurso necesario para la instalación, configuración, operación y mantenimiento de la plataforma, como scripts de automatización, herramientas de desarrollo y archivos de configuración.

La entrega de estos recursos deberá realizarse de manera organizada y estructurada, en un formato que permita al personal técnico de **EL BANCO** comprender y utilizar los mismos sin dificultad. El objetivo es garantizar que el Banco pueda instalar y operar la plataforma de forma autónoma, sin depender de **EL CONTRATISTA** para futuras modificaciones o actualizaciones.
EL CONTRATISTA deberá asegurar que los recursos entregados estén libres de cualquier restricción o dependencia que impida su uso y modificación por parte de **EL BANCO**. Esto incluye la eliminación de cualquier código ofuscado, licencias restrictivas o dependencias de software que no puedan ser adquiridas o utilizadas por el banco.
Los derechos de propiedad intelectual cedidos en virtud a la presente cláusula serán libremente ejercidos y explotados sin restricción por **EL BANCO**, pudiendo este realizar modificaciones o versiones sucesivas del software materia del presente **SERVICIO** y obtener por ello beneficios, salvo y de ser el caso, que se trate de propiedad intelectual de **EL CONTRATISTA**, las cuales deberán estar a nombre de **EL BANCO** y entregadas en el formato oficial de **EL CONTRATISTA**, para dar la conformidad de la entrega, la misma que será verificada por el área técnica especializada o por el área usuaria de **EL BANCO**.

CLÁUSULA DÉCIMA SEGUNDA. - DE LA CONTINUIDAD DEL NEGOCIO

EL CONTRATISTA se compromete a mantener en su organización un esquema de continuidad para la entrega de **EL SERVICIO** contratado por **EL BANCO**, por lo cual deberá contar con un

Plan de Recuperación de Tecnología de Información o, en su defecto, un Plan de Continuidad de Negocio acorde al estándar ISO 22301 o a la Resolución SBS N°877-2020 y sus modificatorias, que contenga procedimientos para responder, recuperar, reanudar y restaurar el nivel de operación predefinido, después de una interrupción del servicio contratado; dicho documento deberá ser entregado a **EL BANCO,** cuando lo solicite, el mismo que deberá encontrarse actualizado y probado cuando menos una vez al año.

Ante la eventual interrupción del **SERVICIO** objeto del contrato por causales imputables a **EL CONTRATISTA**, siempre que dicha interrupción sea por un periodo mayor a cinco (05) minutos, **EL CONTRATISTA** deberá comunicar a **EL BANCO** de forma inmediata o máximo cuatro (4) horas después de ocurrido el incidente, qué origino la interrupción, la cual debe incluir la hora de inicio y fin, en caso que el incidente se encuentre superado; posterior a ello, **EL CONTRATISTA** deberá elaborar un informe el cual debe contener como mínimo fecha, hora, duración, causa/origen, responsabilidad (referida si es **EL CONTRATISTA** u otra empresa asociada que origino la interrupción), estado de los servicio(s) afectado(s), descripción del incidente, acciones de recuperación realizadas, diagnostico general, impacto del servicio, acción de mejora, recomendaciones y conclusiones; el cual debe ser remitido en un plazo máximo de tres (03) días hábiles, periodo contabilizado a partir de la ocurrencia del evento; ambos reportes serán enviados a la Gerencia de Tecnologías de Información de **EL BANCO**.

Asimismo, los cambios que **EL CONTRATISTA** realice a las configuraciones u otros componentes que afecten la operatividad del servicio de objeto del **CONTRATO**, deben ser comunicados a **EL BANCO** con diez (10) días de anticipación a la Gerencia de Tecnología de la Información para su revisión y aprobación.

EL CONTRATISTA se compromete a entregar a **EL BANCO** la documentación y/o información que pueda ser necesaria para el correcto funcionamiento de **EL SERVICIO**, siempre que se establezca de mutuo acuerdo y bajo las consideraciones establecidas en el numeral 6.7 de la **cláusula sexta** de **EL CONTRATO**.

EL CONTRATISTA deberá permitir, facilitar u otorgar a **EL BANCO** la información o revisión que se requiera para el cumplimiento de la cláusula de continuidad del negocio relacionados con **EL SERVICIO** objeto de **EL CONTRATO**.

El incumplimiento de las obligaciones que asume **EL CONTRATISTA** en la presente cláusula constituye causal de resolución automática y de pleno derecho de EL CONTRATO, de conformidad con lo previsto en el artículo 1430° del Código Civil, sin perjuicio de la obligación de **EL CONTRATISTA** de pagar a **EL BANCO** la indemnización correspondiente, y según lo establecido en la cláusula Décima Quinta de EL CONTRATO.

CLAUSULA DÉCIMA TERCERA. – SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

13.1. Para garantizar la integridad, disponibilidad, confidencialidad, privacidad, autenticidad, y trazabilidad de la información; **EL CONTRATISTA** debe cumplir con los lineamientos de seguridad de la información y ciberseguridad; establecidos en las siguientes normativas o su equivalente con los estándares internacionales; en lo que aplique **EL SERVICIO** contratado, como son:

- Resolución SBS N° 504-2021, Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad y sus modificaciones.
- Decreto Supremo N.º 029-2021-PCM, que aprueba el Reglamento del Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital.
- Norma Técnica Peruana NTP- ISO/IEC 27001-2022, Seguridad de la Información, Ciberseguridad y Protección de la Privacidad. Sistemas de Gestión de la Seguridad de la Información. Requisitos.
- Ley N° 29733 - Ley de Protección de Datos Personales, su Reglamento y Directiva de Seguridad.

- Resolución SBS N°6523 – 2013, que aprueba el Reglamento de Tarjetas de Crédito y Débito y sus modificatorias vigentes

13.2. **EL CONTRATISTA** se obliga a adoptar las medidas necesarias para sus trabajadores, representantes y personal o terceros subcontratados que intervengan para el cumplimiento de **EL SERVICIO** contratado, cumplan con las disposiciones sobre la seguridad y confidencialidad de la información.

13.3. **EL CONTRATISTA** es el responsable del resguardo y protección de los activos de información (equipos, dispositivos informáticos, aplicaciones, información, datos, entre otros) de propiedad de **EL BANCO**, involucrados en **EL SERVICIO** contratado, que se encuentren bajo la administración de **EL CONTRATISTA** o que formen parte del servicio contratado.

13.4. **EL BANCO** en coordinación con **EL CONTRATISTA**, adoptarán las medidas de seguridad en los sistemas tecnológicos involucrados en el servicio contratado, a fin de mitigar los riesgos y asegurar que la información se proteja de forma segura, siempre que se hayan establecido dentro del alcance de la solución propuesta. Estas medidas deberán ser plasmadas en un documento y ejecutadas en la etapa de implementación y ante cualquier incidente o mejora del servicio.

13.5. **EL BANCO** y **EL CONTRATISTA** restringirán el acceso a la información física y lógica, así como a los sistemas informáticos inmersos en el servicio; sólo al personal autorizado de **EL BANCO** y **EL CONTRATISTA**, por lo que ningún tercero no autorizado tendrá acceso a la información relacionada con el servicio contratado.

13.6. **EL CONTRATISTA** permitirá, facilitará y/u otorgará a **EL BANCO** la revisión del cumplimiento de las normas de seguridad de la información y ciberseguridad relacionados con el servicio contratado.

CLÁUSULA DÉCIMA CUARTA. - CONFIDENCIALIDAD DE LA INFORMACIÓN

14.1. Cada una de **LAS PARTES** en la ejecución de **EL CONTRATO**, podrá tomar conocimiento de la información de la otra parte. Esta información es confidencial, por lo tanto, en el marco de lo establecido en el Acuerdo de Confidencialidad, que se integra a la firma del presente Contrato, cada parte y todo su personal mantendrá la confidencialidad de la misma. El compromiso de confidencialidad se prolonga por diez (10) años después de terminado **EL CONTRATO**, y se hace extensivo al personal de **EL CONTRATISTA** o aquella que subcontrate, de ser el caso, aun cuando hayan dejado de tener vínculo laboral con dicha parte.

14.2. Cada parte se compromete a mantener toda información suministrada por la otra parte en estricta reserva y absoluta confidencialidad, así como de adoptar las medidas que resulten necesarias para impedir que la Información Confidencial sea conocida o revelada a terceros o que sea utilizada para fines distintos para los cuales fue entregada.

14.3. Cada parte se obliga a tomar todas las medidas y precauciones razonables para que sus trabajadores y en general cualquier persona con la que tenga relación, no divulgue a ningún tercero los documentos o información a los que tengan acceso, haciéndose responsables por la divulgación que se pueda producir y asumiendo el pago de la indemnización por daños y perjuicios. Estas medidas incluyen, aunque no se limitan a: (i) poner en disposición la información confidencial sólo a un número restringido de personas; (ii) permitir que sus trabajadores, agentes o terceros, accedan a la información confidencial sólo hasta donde sea necesario para la prestación de los servicios; (iii) exigir a su personal o trabajadores como condición previa al acceso a la información confidencial que se obliguen por escrito a respetar esta cláusula de confidencialidad.

14.4. Cada parte reconoce que la información que se le entregue procese, facilite o genere en razón a su desempeño y/o ejecución del contrato, se considera un activo de la otra parte, por consiguiente, cada parte se obliga a:

a) Mantener en confidencial dicha información, sin divulgarla, ni entregarla, directa o indirectamente a terceros, sean personas naturales o jurídicas.
b) No usarla para cualquier otro fin que no sea en relación con a su desempeño y/o ejecución del contrato; ni obtener un beneficio propio o de terceros de ella.
c) No entregarla o revelarla, de manera total o parcial, pública o privada, a ninguna persona sea en el Perú como en el extranjero, sin el consentimiento escrito previo de la otra parte, aun cuando se encuentre obligado con alguna de **LAS PARTES** por un acuerdo de confidencialidad similar; salvo a los empleados de cada una de ellas o de cualquier otra persona que se encuentre en una relación contractual o de confianza con dicha parte y que requiera dicha información para utilizarla para asuntos relacionados con los servicios.

Cada parte debe asegurar de que toda la Información Confidencial sea usada para el exclusivo beneficio de los servicios que se prestan en virtud del presente contrato. Por tal razón, la violación de cualquiera de las disposiciones establecidas en esta cláusula obligará a la parte a indemnizar todos los perjuicios directos que cause con motivo de ello, según lo establecido en el numeral 6.12 de la cláusula sexta y, de caso ser necesario, a resolver de manera automática **EL CONTRATO,** de conformidad con lo dispuesto en el artículo 1430° del Código Civil.

14.5. Se considera como violación de la confidencialidad y, por tanto, una conducta desleal, la divulgación o explotación sin autorización de la otra parte, de la información a la que tendrá acceso legítimamente, pero con deber de reserva.

14.6. Se entiende que la obligación asumida está referida no sólo a documentos e informaciones señalados por la otra parte como "confidenciales" sino a todos los documentos e informaciones que, en razón del referido intercambio, pueda ser conocida por cualquier medio, incluyendo sin limitarse a ella, características técnicas, sistemas, programación de instalación, ubicación física, información de las oficinas y demás.

14.7. Cada parte se obliga a mantener y guardar en estricta reserva y absoluta confidencialidad todos los documentos e informaciones que reciban de la otra parte, durante las negociaciones y ejecución del **SERVICIO**.

14.8. Toda información confidencial, utilizada y/o custodiada por **EL CONTRATISTA** para la provisión del **SERVICIO**, deberá ser devuelta a **EL BANCO** en un plazo no mayor a diez (10) días calendarios, así como la eliminación de la información ante la culminación del **SERVICIO.**

CLAUSULA DÉCIMA QUINTA. - PROTECCIÓN DE DATOS PERSONALES, SECRETO BANCARIO Y LAS TELECOMUNICACIONES

15.1. **EL CONTRATISTA**, debe cumplir con el tratamiento de datos personales de acuerdo con las disposiciones establecidas en la Ley N° 29733, Ley de Protección de Datos Personales, su Reglamento, Directiva y sus modificatorias.

15.2. **EL CONTRATISTA**, debe garantizar que los datos personales proporcionados por **EL BANCO** no serán utilizados para otra finalidad que no tenga relación con los servicios contratados.

15.3. **EL CONTRATISTA** se obliga a salvaguardar el secreto bancario y de las comunicaciones sobre la información a la que tiene acceso producto de **EL SERVICIO** contratado, así como garantizar que su personal cumpla con lo establecido en la Ley N° 26702 - Ley General

del Sistema Financiero y del Sistemas de Seguros y Orgánica de la Superintendencia de Banca y Seguros y la Resolución Ministerial N° 111-2009-MTC/03 - Norma que establece medidas destinadas a salvaguardar el derecho a la inviolabilidad y el secreto de las telecomunicaciones y la protección de datos personales, y regula las acciones de supervisión y control a cargo del Ministerio de Transportes y Comunicaciones.

15.4. **EL BANCO**, en caso lo crea necesario, podrá, solicitar con un mínimo de dos (2) días hábiles de anticipación, de forma presencial o electrónica revisar y/o verificar a **EL CONTRATISTA** sobre las medidas de seguridad aplicadas en cumplimiento de la Ley de Protección de Datos Personales, su reglamento, directiva y demás normas conexas, complementarias, modificatorias y/o sustitutorias. De comprobar **EL BANCO** algún incumplimiento por parte de **EL CONTRATISTA** como resultado de la revisión o verificación, previamente enviará una comunicación a **EL CONTRATISTA** comunicándole el incumplimiento debidamente sustentado, y otorgándole un plazo razonable para su cumplimiento, de perseverar **EL CONTRATISTA** en el incumplimiento, **EL BANCO** podrá, interponer las acciones legales que hubiera lugar. En ese sentido, **EL CONTRATISTA** será responsable por cualquier perjuicio que se cause a **EL BANCO** como consecuencia directa o indirecta del incumplimiento de cualquiera de las obligaciones que se desprenden de la presente cláusula de protección de datos personales, y según lo establecido en el numeral 6.12 de la cláusula sexta.

15.5. En caso exista flujo transfronterizo de datos personales, entendiéndose a este como la transferencia internacional de datos personales a un destinatario situado en un país distinto al país de origen de los datos personales, asociados al **SERVICIO** contratado, **EL CONTRATISTA** deberá comunicar a **El BANCO** y asegurarse que la información de datos personales que se transmita y/o transfiera entre el Perú y cualquier otro país, a causa directa o indirecta del servicio contratado; mantiene y mantendrá los niveles de protección adecuados, disponiendo las medidas de seguridad, privacidad y confidencialidad necesarias y efectivas para evitar la adulteración, pérdida, consulta o tratamiento no autorizado de los datos, y que permitan detectar desviaciones, intencionales o no, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado; verificando que todas estas medidas y acciones no sean inferiores a las dispuestas por la Ley N° 29733, su reglamento, directiva de seguridad y normas conexas, de manera tal que garanticen el nivel de seguridad apropiado para abordar los riesgos asociados al tratamiento de datos personales y a la naturaleza sensible de los datos que han de protegerse. En caso **EL BANCO** proporcione a **EL CONTRATISTA** datos personales de sus clientes o usuarios y éste último deba recopilarlos o generarlos, en el marco del cumplimiento del contrato, ello no implicará de modo alguno la transferencia de los mismos, debiendo **EL CONTRATISTA** asumir en dichos casos, la condición de encargado del tratamiento. **EL CONTRATISTA** declara conocer que asume la condición de encargado del tratamiento cuando **EL BANCO** entrega o pone a disposición de manera directa o indirecta a **EL CONTRATISTA** información que contiene datos personales en virtud de una relación jurídica que los vincula.

15.6. **EL CONTRATISTA** declara conocer las sanciones tipificadas en la Ley N° 30096, Ley de Delitos Informáticos (integridad de datos informáticos, tráfico ilegal de datos, interceptación de datos informáticos), y la Ley N° 30171 que modifica la Ley 30096, Ley de Delitos Informáticos, bajo la cual se obliga a dar cumplimiento de estas.

CLÁUSULA DÉCIMA SEXTA. - GESTIÓN INTEGRAL DE RIESGOS

EL CONTRATISTA se obliga a permitir la revisión, supervisión e inspección en lo que aplique a **EL SERVICIO** prestados y de las condiciones que garanticen la seguridad de información, protección de datos personales, continuidad del negocio y gestión de sus riesgos, por parte de la Dependencia Responsable del Contrato, el Órgano de Auditoría Interna de **EL BANCO**, de la Sociedad Auditora Externa, así como por parte de la Superintendencia de Banca, Seguros y AFP, en la oportunidad que cualquiera de estos órganos lo solicite, con un aviso previo por escrito de

veinticuatro (24) horas, el cual será remitido a la dirección indicada por **EL CONTRATISTA** en **EL CONTRATO.**

En dicho comunicado se designarán a las personas que efectuarán la mencionada revisión, supervisión e inspección. Consecuentemente, **EL CONTRATISTA** se compromete a facilitar todos los recursos y medios necesarios a las personas antes mencionadas para efectuar dicha revisión.

El incumplimiento de las obligaciones que asume **EL CONTRATISTA** en las cláusulas relacionadas con los temas a que se refiere el primer párrafo de la presente cláusula, constituye causal de resolución automática y de pleno derecho del presente contrato, de conformidad con lo previsto en el artículo 1430° del Código Civil, sin perjuicio de la obligación de **EL CONTRATISTA** de pagar a **EL BANCO** la indemnización correspondiente, y según lo establecido en el numeral 6.12 de la cláusula sexta.

En caso **EL BANCO** incurriera en costos y/o multas establecidas por parte de un organismo regulador u otro, producto de la interrupción y/o algún error o falla en las condiciones de la prestación del servicio por causas imputables a **EL CONTRATISTA**, éste se hará totalmente responsable de dichas penalidades, costos y/o multas, asumiendo el importe de las mismas sin reserva ni limitación alguna. Por lo que **EL BANCO**, podrá evaluar la aplicación de penalidades o el pago de indemnización mediante las cláusulas de penalidades que correspondan por la no operatividad del **SERVICIO**, conforme a el(los) SLA que se haya(n) definido en el **Anexo N° 01**.

CLÁUSULA DÉCIMA SÉPTIMA. - GESTION INTEGRAL DE RIESGO OPERATIVO Y AUDITORIA

EL CONTRATISTA debe implementar y cumplir con los lineamientos definidos por **EL BANCO** en cumplimiento a la Resolución SBS N° 272-2017 "Reglamento de Gobierno Corporativo y de la Gestión Integral de Riesgos" y "Reglamento para la Gestión del Riesgo Operacional" aprobado por Resolución SBS N° 2116-2009, cumpliendo con lo siguiente:

17.1. **EL CONTRATISTA**, de acuerdo con el tamaño, naturaleza y complejidad de su negocio, deberá contar obligatoriamente con un proceso orientado a gestionar el riesgo operacional aplicables al SERVICIO brindado a **EL BANCO**, que permita identificar, evaluar, tratar, medir, controlar, monitorear y reportar los diversos riesgos que enfrentan, siendo responsable frente a este último en caso de culpa o negligencia.

17.2. **EL CONTRATISTA** deberá brindar a **EL BANCO**, la información que éste pueda requerir para implementar las medidas que sirvan controlar el cumplimiento de la presente cláusula de riesgo de operación.

17.3. **EL CONTRATISTA** deberá comunicar formalmente a **EL BANCO**, un reporte periódico que evidencie la gestión de riesgos en las operaciones o servicios prestados.

El incumplimiento de las obligaciones que asume **EL CONTRATISTA** en la presente cláusula constituye causal de resolución automática y de pleno derecho de EL CONTRATO, de conformidad con lo previsto en el artículo 1430° del Código Civil, sin perjuicio de la obligación de **EL CONTRATISTA** de pagar a **EL BANCO** la indemnización correspondiente, según lo establecido en el numeral 6.12 de la cláusula sexta

CLÁUSULA DÉCIMA OCTAVA: PREVENCIÓN DE LAVADO DE ACTIVOS Y ANTICORRUPCIÓN/ANTISOBORNO

18.1. **EL BANCO** es responsable de asegurar el cumplimiento de la normatividad emitida por la Superintendencia de Banca, Seguros y AFPs (SBS), por lo que **EL CONTRATISTA** declara conocerlo y se obliga a facilitar a **EL BANCO** previo a la firma del presente **CONTRATO** y durante la vigencia del mismo, en la oportunidad y a solo requerimiento de

EL BANCO, toda la información y documentación referida a las actividades comerciales de **EL CONTRATISTA**, así como de sus socios y/o accionistas y/o representantes legales.

18.2. Dicha información comprenderá como mínimo el formato currículo vitae, ficha RUC, vigencia de poderes y/o copia literal de la partida, copia de los documentos de identidad de los accionistas y representante legal, estados financieros; así como cualquier otra documentación que se requiera para cumplir con la debida diligencia de Contrapartes y Gestión de los Riesgos de LA/FT a los que se encuentra expuestos **EL BANCO**, sin que esta enumeración resulte limitativa. Ante el requerimiento por parte de **EL BANCO**, **EL CONTRATISTA** se obliga a proporcionar la información en un plazo razonable. Asimismo, **LAS PARTES** establecen que la información requerida solo podrá versar sobre la referente al presente contrato o toda aquella que pueda generar un impacto importante respecto de lo establecido en la presente cláusula.

18.3. **EL CONTRATISTA** declara que los fondos con los que se conformó el capital de la empresa se originaron en negocios lícitos, que todas las actividades e ingresos que se perciben provienen de actividades lícitas; y que, ni **EL CONTRATISTA**, ni sus socios y/o accionistas, ni su representante legal, se encuentra/n en ninguna lista de reportes internacionales, nacionales o bloqueados por actividades de narcotráfico, lavado de activos o terrorismo. Asimismo, declara que tampoco existe en su contra, ni sus socios y/o accionistas, ni su representante legal ningún procedimiento o proceso en instancias nacionales o internacionales por ninguno de los aspectos anteriores. Por lo que, **EL CONTRATISTA** reconoce que de incurrir en alguna/s de la/s situación/es previstas en este párrafo, el presente contrato quedará resuelto de forma automática.

18.4. Asimismo, en relación con el cumplimiento de las obligaciones derivadas del presente Contrato, **EL CONTRATISTA** declara estar de acuerdo y garantiza que:

a) No ha violado y no violará las leyes vigentes de lucha contra el lavado de activos, financiamiento del terrorismo, corrupción y sus regulaciones.
b) No ha realizado, y se compromete a no realizar o a participar en las siguientes conductas: realización de pagos o transferencias de valor, ofertas, promesas o la concesión de cualquier ventaja económica o de otro tipo, solicitudes, acuerdos para recibir o aceptar cualquier ventaja financiera o de otro tipo, ya sea directa o indirectamente, que tenga el propósito, el efecto, la aceptación o la conformidad del soborno público o comercial o cualquier otro medio ilegal o indebido de obtener o retener un negocio, una ventaja comercial o de la mala ejecución de cualquier función o actividad.
c) Deberá procurar el cumplimiento de las obligaciones mencionadas en los literales a) y b) de sus propios asociados, agentes o subcontratistas que puedan ser utilizados por **EL CONTRATISTA** para el cumplimiento de las obligaciones en virtud del presente contrato.
d) **EL CONTRATISTA** deberá contar con políticas y procedimientos diseñados para prevenir la existencia de actos que puedan calificar como lavado de activos, terrorismo, soborno o corrupción en la ejecución del presente contrato, **EL CONTRATISTA** deberá cumplir estas obligaciones a partir de sus propias personas, asociadas, agentes o subcontratistas que puedan ser utilizados en la ejecución del presente contrato.

18.5. En caso de que **EL CONTRATISTA** tuviera noticia de la ocurrencia de alguno de estos hechos en el marco del presente **CONTRATO** que actual o potencialmente pudieran impactar de cualquier forma a **EL BANCO** sea en su responsabilidad penal, civil o crédito y reputación, deberá informar de inmediato de este hecho a **EL BANCO**; sin perjuicio de tomar todas las medidas necesarias para evitar o mitigar estos efectos. Asimismo, **EL CONTRATISTA** se compromete a entregar a **EL BANCO** toda la información que éste le requiera en el marco de las investigaciones internas, sean éstas de carácter meramente preventivo o cuándo se indague sobre hechos constitutivos de delito, sea que estas investigaciones tengan carácter sistemático o aleatorio.

18.6. El incumplimiento de las obligaciones asumidas por **EL CONTRATISTA** a través de la

presente clausula, constituye causal de resolución automática del presente contrato, siendo responsable **EL CONTRATISTA**, de todas las multas y sanciones impuestas a **EL BANCO** derivadas directamente de este tipo de incumplimientos, según lo establecido en el numeral 6.12 de la cláusula sexta.

18.7. **EL BANCO** sólo contrata con quienes mantengan los más altos estándares de honestidad, ética y profesionalismo en la gestión de sus negocios. **EL BANCO** toma muy en serio e investigará cualquier indicio, denuncia, sugerencia o evidencia que indique que **EL CONTRATISTA** pueda estar involucrada en prácticas prohibidas o indebidas de corrupción, o en caso éste haya ejercitado actos coercitivos indebidos, incentivos indebidos, ofertas indebidas, chantaje o violencia, para obtener ventaja contractual. Estas son prácticas que **EL BANCO** rechaza, por lo que **EL BANCO** no efectúa ningún tipo de negocio o contrato con aquellas organizaciones que se gestionen con esas prácticas indebidas. En caso **EL BANCO** descubra que **EL CONTRATISTA** está involucrado en tales prácticas, **EL BANCO** estará facultada para resolver de inmediato el contrato y podrá retener los montos comprometidos en tales prácticas indebidas. Esta disposición será aplicada en todo su rigor.

18.8. En particular, **EL BANCO** prohíbe expresamente a todos sus proveedores de realizar ofrecimientos, o prometer cualquier pago ilegal, impropio o indebido, o transferir cualquier bien o valor a favor de cualquier autoridad (nacional, regional o local}, tercera parte, o trabajador de **EL BANCO**, a fin de sostener o entablar negocios con **EL BANCO**. **EL BANCO** exige asimismo que toda documentación que le sea remitida, incluyendo la documentación por reembolso de gastos o facturas sean completas y ajustadas a los montos reales y acordes con la naturaleza de los servicios prestados o gastos incurridos. **EL CONTRATISTA** acuerda en cooperar con **EL BANCO** en remitirle cualquier documentación o justificación derivada del contrato que le sea requerida a **EL CONTRATISTA** sobre el particular. **EL BANCO** no realizará pagos a **EL CONTRATISTA** contra facturas o solicitudes de pago que no estén debidamente sustentados.

18.9. **EL CONTRATISTA** garantiza que, en relación con el presente contrato, no ha realizado, directa o indirectamente, ofrecimiento o promesa indebida, irregular, ilícita o ilegal alguna, y se obliga a no realizar ofrecimiento alguno o promesa, pago o transferencia ilícita de cualquier valor o bien, a cualquier autoridad, terceras partes, o trabajadores de **EL BANCO**; y, asimismo, **EL CONTRATISTA** se obliga a cumplir con las normas legales aplicables a la ejecución del presente contrato. El incumplimiento de estas obligaciones o la remisión de información falsa, darán lugar a la resolución inmediata del contrato, sin perjuicio de los demás recursos y remedios establecidos en el presente contrato.

18.10. A la suscripción del presente **CONTRATO**, **EL CONTRATISTA** deberá presentar la siguiente información:

- Nombres y apellidos completos o denominación o razón social, el caso se trate de una persona jurídica.
- Registro Único de Contribuyentes (RUC), o registro equivalente para no domiciliados, de ser el caso.
- Tipo o número de documento de Identidad, en caso de trate de una persona natural.
- Dirección de la oficina o local principal.
- Años de experiencia en el mercado.
- Rubros en los que EL CONTRATISTA brinda sus productos o servicios.
- Identificación de los accionistas, socios o asociados que tengan directa o indirectamente el 25 % del capital social, aporte o participación de la persona jurídica y del nombre del representante legal, considerando la información requerida para las personas naturales.
- Declaración Jurada de no contar con antecedentes penales dEL CONTRATISTA, de ser el caso.

- No encontrarse incluido en la lista emitida por la Oficina de Control de Activos Extranjeros del Departamento de Tesoro de los Estados Unidos de América (OFAC).

CLÁUSULA DÉCIMA NOVENA. - SEGURIDAD Y SALUD EN EL TRABAJO

EL CONTRATISTA, a la suscripción del **CONTRATO** deberá presentar obligatoriamente una declaración jurada que cumple las disposiciones establecidas en la Ley N° 29783 – Ley de Seguridad y Salud en el Trabajo y su Reglamento.

CLÁUSULA VIGÉSIMA. - REGISTRO DE DEUDORES DE REPARACIÓN CIVIL - REDERECI

A la suscripción del **CONTRATO**, **EL CONTRATISTA** deberá presentar Declaración Jurada de no encontrarse inscritos en el Registro de Deudores de Reparación Civil.

CLÁUSULA VIGESIMA PRIMERA. - LEY APLICABLE Y SOLUCIÓN DE CONTROVERSIAS

El presente Contrato se encuentra sujeto a las disposiciones de la Ley Nº26702, el Código Civil y a cualquier otra disposición vigente que resulte aplicable.

Todo litigio, controversia, desavenencia, reclamación o interpretación resultante, o relacionada o derivada de este Contrato o que guarde relación con él, incluidas las relativas a su nulidad, validez, eficacia o terminación incluso las del convenio de arbitraje serán resueltas mediante conciliación y/o arbitraje de Derecho ante la Cámara de Comercio de Lima, de conformidad con los reglamentos de dicho Centro.

Si la conciliación concluyera por inasistencia de una o ambas partes, con un acuerdo parcial o sin acuerdo, **LAS PARTES** se someterán a un Arbitraje de Derecho para que resuelvan las controversias definitivamente. No es obligatoria la conciliación previa al Arbitraje.

El arbitraje antes referido tendrá las siguientes características y regulaciones:

- ✓ El arbitraje será de derecho e institucional, bajo la administración de la Cámara de Comercio de Lima, a cuyos reglamentos y estatutos **LAS PARTES** acuerdan someterse en forma expresa e irrevocable. El arbitraje será en Lima y en idioma español, y bajo las leyes peruanas.
- ✓ En caso de que el monto de la cuantía de la solicitud de arbitraje sea menor a 50 (cincuenta) Unidades Impositivas Tributarias - UIT, vigentes a la fecha de la solicitud, la controversia será resuelta por Árbitro Único designado por la Cámara de Comercio de Lima.
- ✓ En caso de que el monto de la cuantía de la solicitud de arbitraje sea mayor o igual a 50 (cincuenta) Unidades Impositivas Tributarias - UIT, vigentes a la fecha de la solicitud, la controversia será resuelta por un Tribunal compuesto por tres (03) árbitros.
- ✓ Cada parte interviniente designará un árbitro y los dos árbitros designados escogerán al Presidente del Tribunal, a falta de acuerdo de los dos árbitros para escoger al Presidente, éste será designado por la Cámara de Comercio de Lima.
- ✓ **LAS PARTES** acuerdan que respecto a los honorarios de los árbitros y del Presidente del Tribunal Arbitral, cada parte interviniente asumirá el costo de los honorarios del Árbitro que designe y además asumirá el 50% de los honorarios del Presidente del Tribunal Arbitral, de darse el caso, salvo el referente a los honorarios de los abogados que serán asumidos por cada una de **LAS PARTES.**
- ✓ El laudo arbitral emitido obligará a **LAS PARTES** y pondrá fin al procedimiento de manera definitiva, siendo el mismo inapelable ante el Poder Judicial o cualquier instancia administrativa, tiene el valor de cosa juzgada y se ejecutará como una sentencia. Queda perfectamente entendido que **LAS PARTES** no le confieren al Tribunal o al Árbitro Único la posibilidad de ejecutar el laudo.

En el caso que **LAS PARTES** o el árbitro tuvieran que recurrir al Poder Judicial, queda establecido que, en estos casos, serán competentes los jueces y tribunales del distrito judicial de

Lima, Perú, renunciando **LAS PARTES** al fuero de los jueces que les pudiera corresponder por razón de su domicilio.

Queda entendido que los acuerdos contenidos en la presente Cláusula sobrevivirán a la terminación o resolución del presente Contrato y serán aplicables a cualquier conflicto que pudiera generarse entre **LAS PARTES** con relación al presente Contrato y los derechos y obligaciones que se deriven de éste, incluyendo los conflictos derivados o relativos a su extinción, salvo acuerdo distinto y posterior de **LAS PARTES.**

CLÁUSULA VIGÉSIMA SEGUNDA. - DOMICILIO PARA EFECTOS DE LAS COMUNICACIONES Y EJECUCIÓN CONTRACTUAL

LAS PARTES declaran el siguiente domicilio para efecto de las notificaciones que se realicen durante la ejecución de **EL CONTRATO**:

DOMICILIO DEL BANCO: Avenida Javier Prado Este Nº 2499 San Borja - Lima

DOMICILIO DEL CONTRATISTA: [.....]

La variación del domicilio aquí declarado de alguna de **LAS PARTES** debe ser comunicada a la otra parte, formalmente y por escrito, con una anticipación no menor de quince (15) días calendario.

De acuerdo con las bases integradas, la oferta y las disposiciones del presente **CONTRATO**, **LAS PARTES** lo firman por duplicado en señal de conformidad en la ciudad de Lima a los […] del mes de [……..…] del año 202[..].

EL BANCO	EL CONTRATISTA

EL BANCO

Anexo N°01
TÉRMINOS DE REFERENCIA – TDR

Anexo N°02
PROPUESTA TÉCNICA DE EL CONTRATISTA

Formatos

Formato N° 1

DECLARACIÓN JURADA DE DATOS DEL POSTOR

Señores
COMITÉ DEL CONCURSO DE MERITOS
Concurso de Méritos Nº 0004-2024-BN
Presente.-

El que se suscribe, [……..], Representante Legal de [……], identificado con [CONSIGNAR TIPO DE DOCUMENTO DE IDENTIDAD] N° [CONSIGNAR NÚMERO DE DOCUMENTO DE IDENTIDAD], con poder inscrito en la localidad de en la Ficha Nº [……] Asiento Nº [……], **DECLARO BAJO JURAMENTO** que la siguiente información se sujeta a la verdad:

Razón Social :			
Domicilio Legal :			
RUC :	Teléfono(s) :		
Correo electrónico :			

Autorización de notificación por correo electrónico:

… [CONSIGNAR SÍ O NO] autorizo que se notifiquen al correo electrónico indicado las siguientes actuaciones:

1. Solicitud de la descripción a detalle de todos los elementos constitutivos de la oferta.
2. Solicitud de subsanación de los requisitos para perfeccionar el contrato.
3. Solicitud al postor que ocupó el segundo lugar en el orden de prelación para presentar los documentos para perfeccionar el contrato.

Asimismo, me comprometo a remitir la confirmación de recepción, en el plazo máximo de dos (2) días hábiles de recibida la comunicación.

[CONSIGNAR CIUDAD Y FECHA]

…….....
Firma, Nombres y Apellidos del postor o
Representante legal, según corresponda

Importante

La notificación dirigida a la dirección de correo electrónico consignada se entenderá válidamente efectuada.

Importante
Cuando se trate de consorcios, la declaración jurada es la siguiente:

Formato N° 1

DECLARACIÓN JURADA DE DATOS DEL POSTOR

Señores
COMITÉ DEL CONCURSO DE MERITOS
Concurso de Méritos Nº 0004-2024-BN
Presente.-

El que se suscribe, [……..], representante común del consorcio [CONSIGNAR EL NOMBRE DEL CONSORCIO], identificado con [CONSIGNAR TIPO DE DOCUMENTO DE IDENTIDAD] N° [CONSIGNAR NÚMERO DE DOCUMENTO DE IDENTIDAD], **DECLARO BAJO JURAMENTO** que la siguiente información se sujeta a la verdad:

Datos del consorciado 1			
Razón Social :			
Domicilio Legal :			
RUC :	Teléfono(s) :		
Correo electrónico :			

Datos del consorciado 2			
Razón Social :			
Domicilio Legal :			
RUC :	Teléfono(s) :		
Correo electrónico :			

Datos del consorciado …			
Razón Social :			
Domicilio Legal :			
RUC :	Teléfono(s) :		
Correo electrónico :			

Autorización de notificación por correo electrónico:

Correo electrónico del consorcio:

……. [CONSIGNAR SÍ O NO] autorizo que se notifiquen al correo electrónico indicado las siguientes actuaciones:

1. Solicitud de la descripción a detalle de todos los elementos constitutivos de la oferta.
2. Solicitud de subsanación de los requisitos para perfeccionar el contrato.
3. Solicitud al postor que ocupó el segundo lugar en el orden de prelación para presentar los documentos para perfeccionar el contrato.

Asimismo, me comprometo a remitir la confirmación de recepción, en el plazo máximo de dos (2) días hábiles de recibida la comunicación.

[CONSIGNAR CIUDAD Y FECHA]

……..……..

Firma, Nombres y Apellidos del representante común del consorcio

Importante

La notificación dirigida a la dirección de correo electrónico consignada se entenderá válidamente efectuada.

Formato N° 2

DECLARACIÓN JURADA PARA SER POSTOR

Señores
COMITÉ DEL CONCURSO DE MERITOS
Concurso de Méritos Nº 0004-2024-BN
Presente.-

Mediante el presente el suscrito, postor y/o Representante Legal de [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA], declaro bajo juramento:

i. No haber incurrido y me obligo a no incurrir en actos de corrupción, así como a respetar el principio de integridad.

ii. No tener impedimento para postular en el proceso de concurso de méritos ni para contratar con el Estado.

iii. Que mi información (en caso que el postor sea persona natural) o la información de la persona jurídica que represento, registrada en el RNP se encuentra actualizada.

iv. Conocer las sanciones contenidas en la Ley de Contrataciones del Estado y su Reglamento, así como las disposiciones aplicables del TUO de la Ley N° 27444, Ley del Procedimiento Administrativo General.

v. Participar en el presente proceso de contratación en forma independiente sin mediar consulta, comunicación, acuerdo, arreglo o convenio con ningún proveedor; y, conocer las disposiciones del Decreto Legislativo Nº 1034, Decreto Legislativo que aprueba la Ley de Represión de Conductas Anticompetitivas.

vi. Conocer, aceptar y someterme a las bases, condiciones y reglas del proceso de concurso de méritos.

vii. Ser responsable de la veracidad de los documentos e información que presento en el presente proceso de concurso de méritos.

viii. Comprometerme a mantener la oferta presentada durante el proceso de concurso de méritos y a perfeccionar el contrato, en caso de resultar favorecido con la buena pro.

[CONSIGNAR CIUDAD Y FECHA]

……..
Firma, Nombres y Apellidos del postor o Representante legal, según corresponda

Importante
En el caso de consorcios, cada integrante debe presentar esta declaración jurada, salvo que sea presentada por el representante común del consorcio.

Formato Nº 3

DECLARACIÓN JURADA DE CUMPLIMIENTO DE LOS REQUISITOS, CARACTERISTICAS Y CONDICIONES TECNICAS

Señores
COMITÉ DEL CONCURSO DE MERITOS
Concurso de Méritos Nº 0004-2024-BN
Presente.-

Es grato dirigirme a usted, para hacer de su conocimiento que luego de haber examinado las bases y demás documentos del proceso de concurso de méritos de la referencia y, conociendo todos los alcances y las condiciones detalladas en dichos documentos, el postor que suscribe ofrece el **Servicio de implementación de nueva plataforma bancaria para canales digitales banca móvil y banca por internet del Banco de la Nación**, de conformidad con los requisitos, características y condiciones técnicas que se indican en los Términos de Referencia de las bases, así como los documentos derivados del proceso de concurso de méritos que establezcan obligaciones para las partes.

[CONSIGNAR CIUDAD Y FECHA]

……..
Firma, Nombres y Apellidos del postor o
Representante legal o común, según corresponda

Formato **Nº 4**

DECLARACIÓN JURADA DE PLAZO DE PRESTACIÓN DEL SERVICIO

Señores
COMITÉ DEL CONCURSO DE MERITOS
Concurso de Méritos Nº 0004-2024-BN
Presente.-

Mediante el presente, con pleno conocimiento de las condiciones que se exigen en las bases del proceso de concurso de méritos de la referencia, me comprometo a prestar el servicio objeto del presente proceso de concurso de méritos en el plazo:

Desarrollo de la Aplicación

El plazo de contratación del servicio de la nueva plataforma bancaria para los canales digitales Banca Móvil y Banca por Internet del Banco de la Nación será de **420 días** calendarios. El inicio de la contraprestación del servicio será a partir del día siguiente de aprobado el **Plan de Trabajo**.

Servicios de Nube

El plazo de contratación de lo servicio de nube para la nueva plataforma bancaria para los canales digitales Banca Móvil y Banca por Internet del Banco de la Nación será de **36 meses** como máximo. El inicio de la contraprestación del servicio será a partir del día siguiente de aprobado el **Plan de Trabajo**.

Servicio de Asistencia para Alcanzar la Mejora Continua de la Solución

El servicio de Mejora Continua (ver numeral 33. Mejora Continua del Servicio) tendrá una duración de **90 días calendarios** bajo la modalidad de bolsa de trabajo que considera 600 horas mensuales (total del servicio 1,800 horas), terminado el periodo de 90 días, el servicio tendrá la modalidad a demanda durante el tiempo de ejecución del contrato.

El inicio del servicio de Mejora Continua empezará al día siguiente de la suscripción del Acta de Conformidad correspondiente al MVP 4.

[CONSIGNAR CIUDAD Y FECHA]

……
Firma, Nombres y Apellidos del postor o
Representante legal o común, según corresponda

Formato **Nº 5**

PROMESA DE CONSORCIO

(Sólo para el caso en que un consorcio se presente como postor)

Señores
COMITÉ DEL CONCURSO DE MERITOS
Concurso de Méritos Nº 0004-2024-BN
Presente.-

Los suscritos declaramos expresamente que hemos convenido en forma irrevocable, durante el lapso que dure el proceso de concurso de méritos, para presentar una oferta conjunta al **CONCURSO DE MERITOS N° 0004-2024-BN.**

Asimismo, en caso de obtener la buena pro, nos comprometemos a formalizar el contrato de consorcio, bajo las siguientes condiciones:

a) Integrantes del consorcio

1. [NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL CONSORCIADO 1].
2. [NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL CONSORCIADO 2].

b) Designamos a [CONSIGNAR NOMBRES Y APELLIDOS DEL REPRESENTANTE COMÚN], identificado con [CONSIGNAR TIPO DE DOCUMENTO DE IDENTIDAD] N° [CONSIGNAR NÚMERO DE DOCUMENTO DE IDENTIDAD], como representante común del consorcio para efectos de participar en todos los actos referidos al proceso de concurso de méritos, suscripción y ejecución del contrato correspondiente con [CONSIGNAR NOMBRE DE LA ENTIDAD].

c) Asimismo, declaramos que el representante común del consorcio no se encuentra impedido, inhabilitado ni suspendido para contratar con el Estado.

d) Fijamos nuestro domicilio legal común en [.....].

e) Las obligaciones que corresponden a cada uno de los integrantes del consorcio son las siguientes:

1.	OBLIGACIONES DE [NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL CONSORCIADO 1] [DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 1]	: %][22]
2.	OBLIGACIONES DE [NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL CONSORCIADO 2] [DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 2]	%][23]
	TOTAL OBLIGACIONES	**100 %**][24]

[22] Consignar únicamente el porcentaje total de las obligaciones, el cual debe ser expresado en número entero, sin decimales.
[23] Consignar únicamente el porcentaje total de las obligaciones, el cual debe ser expresado en número entero, sin decimales.
[24] Consignar únicamente el porcentaje total de las obligaciones, el cual debe ser expresado en número entero, sin decimales.

[CONSIGNAR CIUDAD Y FECHA]

…….	……..
Consorciado 1 **Nombres, apellidos y firma del Consorciado 1 o de su Representante Legal** **Tipo y N° de Documento de Identidad**	**Consorciado 2** **Nombres, apellidos y firma del Consorciado 2 o de su Representante Legal** **Tipo y N° de Documento de Identidad**

Importante
Las firmas de los integrantes del consorcio deben ser legalizadas.

Formato **Nº 6**

PRECIO DE LA OFERTA

Señores
COMITÉ DEL CONCURSO DE MERITOS
Concurso de Méritos Nº 0004-2024-BN
Presente.-

Es grato dirigirme a usted, para hacer de su conocimiento que, de acuerdo con las bases, mi oferta es la siguiente:

Formato de Cotización Consolidada

Implementación de la Nueva Plataforma Bancaria para los Canales Digitales Banca Móvil y Banca por Internet del Banco de la Nación

Implementación de la Nueva Plataforma Bancaria para los Canales Digitales Banca Móvil y Banca por Internet del Banco de la Nación Costo según Conceptos del Servicio	**Costo (S/ inc. IGV)**
Costo del Servicio de Implementación del Proyecto (Anexo N° 1)	
Costo Servicio de Infraestructura en Nube según Componente Tecnológico (Anexo N° 3)	
Costo del Componente Opcional - Cuenta DNI (Anexo N° 4)	
Costo Total del Servicio (S/ inc. IGV)	**0.00**

Anexo N° 1
Costo de Servicio de Implementación del Proyecto
Implementación de la Nueva Plataforma Bancaria para los Canales Digitales Banca Móvil y Banca por Internet del Banco de la Nación

Concepto	Descripción	Costo (S/ inc. IGV)
Diseño, Desarrollo e Implementación de la Solución (21.1)	Incluye diseño de interfaz, desarrollo e implementación de las funcionalidades de la Banca Móvil y Banca por Internet descritas en el numeral 7. Alcance y Descripción del Servicio y en el numeral 13. Desarrollo de APIs	
Implementación de la Infraestructura (21.2.b.1)	Despliegue base para los ambientes	
	Despliegue del ambiente de desarrollo (DEV)	
	Despliegue del ambiente de Calidad (QA)	
	Despliegue del ambiente de Producción (PRD)	
Implementación del Ambiente de Seguridad (21.2.b.2.)	Servicio de implementación Plataforma de protección para aplicaciones CNAPP	
	Servicio Implementación Firewall	
	Servicio Implementación SaaS de Seguridad para los servicios WAF, ataques volumétricos de denegación de servicio y servicio de seguridad de API discovery	
	Servicio Implementación para el Servicio de Detección Avanzada para ataques de Bots Automatizados	
Servicio de Soporte Técnico (21.2.b.4.)	Soporte técnico para la atención y resolución de todos los problemas que se presenten con la solución propuesta	
Servicio de Asistencia para Alcanzar la Mejora Continua de la Solución (21.2.b.4.)	Tendrá una duración de 90 días calendarios bajo la modalidad de bolsa de trabajo que considera 600 horas mensuales (total del servicio 1,800 horas).	Costo Total: S/
		Costo Hora: S/
Total Costos Fijos (S/ inc. IGV)		**0.00**

ANEXO N° 2

Tarifarios según Componente Tecnológico de la Infraestructura en Nube

Implementación de la Nueva Plataforma Bancaria para los Canales Digitales Banca Móvil y Banca por Internet del Banco de la Nación

1. Detallar los rangos de uso para cada componente de la solución, como el almacenamiento en la nube, el procesamiento de datos, la transferencia de datos y otros servicios relevantes.
2. Los proveedores en la descripción presentada en el formato, deben describir en forma clara y concisa el Componente definido por el Banco de la Nación o renombrado de acuerdo a su Solución propuesta.
3. Especificar claramente los límites de uso para cada componente, indicando el volumen máximo de transacciones contemplado en cada rango, para el presente servicio se ha establecido un total de cinco (05) rangos, de menor a mayor, por componente. En caso de que el componente tenga un solo valor, el proveedor deberá considerarlo como valor único y definirlo en la columna "Descripción"
4. Proporcionar una descripción de cómo se calcularán y aplicarán los precios por transacción dentro de cada rango de uso.
5. Asegurarse de que los rangos de uso propuestos sean adecuados y estén alineados con las necesidades del proyecto, garantizando la escalabilidad de la solución a lo largo del tiempo.
6. Presentar la información de manera clara y concisa en la propuesta, asegurándose de que sea fácilmente comprensible para el Comité Evaluador.
7. Los proveedores podrán añadir más componentes, según su Solución propuesta.
8. Los proveedores podrán redefinir la denominación de sus Componentes presentados en el Anexo, con la denominación de los Componentes que su Solución propuesta defina.

Ítem	Componente	Descripción	Unidad de Medida	Rango de Uso Mensual	Costo Unitarios (S/ Inc. IGV)
10.1. Servicios Compartidos					
1	Servicio de NAT Horas				
2	Conexión VPN Site to Site				
3	Conexión Cliente VPN				
4	Conector de redes en múltiples zonas				
5	Servicio de transferencia de datos				
6	Kit de desarrollo de software en la nube				
7	Servicio de entrega continua				
8	Repositorio de paquetes de software				
9	Servicio de construcción e integración continua con Sistema operativo Linux.				
10	Recurso de cómputo con las siguientes características: 8 vCPU y 16 GB Memoria				
11	Registro de contenedores				
12	Servicio de autenticación Web/móvil				
13	Servicio de logs de la consola en nube				
10.2. Ambiente de Producción					
1	Servicio de base de datos relacional compatible con PostgreSQL en alta disponibilidad (Primario/Respaldo) en multizona				
2	Cada característica puede consumirse de manera independiente				
3	Servicio de base de datos de documentos compatible con (mongoDB) Cada característica puede consumirse de manera				

	independiente 2 Instancias, una por Zona de disponibilidad				
4	Servicio de administración y despliegue de APIs				
5	Balanceador de carga de red				
6	Servicio de contenedores basado en Kubernetes				
7	Servicio de máquinas virtuales de cómputo para kubernetes con Sistema operativo Linux				
8	Servicio de CDN				
9	Servicio de gestión de claves criptográficas				
10	Servicio de almacenamiento de secretos				
11	Servicio de almacenamiento de objetos				
12	Servicio de monitoreo y observabilidad				
13	SFTP				
14	Servicio de ejecución de Funciones sin servidor				
10.3. Ambiente de Certificación (QA)					
1	Servicio de base de datos relacional compatible con PostgreSQL en alta disponibilidad (Primario/Respaldo) en multizona				
2	Servicio de base de datos de documentos compatible con (mongoDB) Cada característica puede consumirse de manera independiente 2 Instancias, una por Zona de disponibilidad				
3	Servicio de administración y despliegue de APIs				
4	Balanceador de carga de de aplicación				
5	Servicio de contenedores basado en Kubernetes				
6	Servicio de máquinas virtuales de cómputo con Sistema operativo Linux				
7	Servicio de CDN				
8	Servicio de gestión de claves criptográficas				
9	Servicio de almacenamiento de secretos				
10	Servicio de almacenamiento de objetos				
11	Servicio de monitoreo y observabilidad				
12	SFTP				
13	Servicio de ejecución de Funciones sin servidor				
10.4. Ambiente Desarrollo (DEV)					

1	Servicio de base de datos relacional compatible con PostgreSQL				
2	Servicio de base de datos de documentos compatible con (mongoDB) Servicio de administración y despliegue de APIs				
3	Balanceador de carga de aplicación				
4	Servicio de contenedores basado en Kubernetes				
5	Servicio de máquinas virtuales de cómputo con Sistema operativo Linux				
6	Servicio de CDN				
7	Servicio de gestión de claves criptográficas				
8	Servicio de almacenamiento de secretos				
9	Servicio de almacenamiento de objetos				
10	Servicio de monitoreo y observabilidad				
11	SFTP				
12	Servicio de ejecución de Funciones sin servidor				
10.5. Componentes a Demanda					
1	Servicio de base de datos relacional (HA)				
2	Servicio de base de datos de documentos				
3	Servicio de máquinas virtuales de cómputo para kubernetes con Sistema operativo Linux				
4	Direct Connet hosteado				
11.8. Especificaciones de Capacidades de los Servicios de Seguridad					
1	Consola SaaS de Seguridad para los servicios WAF, ataques volumétricos de denegación de servicio y servicio de seguridad de APIs.				
2	Plataforma de protección nativa de nube para aplicaciones (CNAPP)				
3	Servicio de Next Generation Firewall (NGFW)				

Ejemplo: Tarifarios de Componentes

Ítem	Componente	Descripción	Unidad de medida	Rango de uso mensual	Costo Unitarios (S/ Inc. IGV)
10.1. Servicios Compartidos					
1	Servicio de NAT Horas			1 hasta <…>	
				<…> hasta <…>	
				<…> hasta <…>	
				<…> hasta <…>	
				Más de <…>	
2	Conexión VPN Site to Site			1 hasta <…>	
				<…> hasta <…>	
				<…> hasta <…>	
				<…> hasta <…>	

				Más de <…>	
3	Conexión Cliente VPN			1 hasta <…>	
				<…> hasta <…>	
				<…> hasta <…>	
				<…> hasta <…>	
				Más de <…>	
4	Conector de redes en múltiples zonas			1 hasta <…>	
				<…> hasta <…>	
				<…> hasta <…>	
				<…> hasta <…>	
				Más de <…>	
5	Servicio de transferencia de datos			1 hasta <…>	
				<…> hasta <…>	
				<…> hasta <…>	
				<…> hasta <…>	
				Más de <…>	
6	Kit de desarrollo de software en la nube			1 hasta <…>	
				<…> hasta <…>	
				<…> hasta <…>	
				<…> hasta <…>	
				Más de <…>	
7	Servicio de entrega continua			1 hasta <…>	
				<…> hasta <…>	
				<…> hasta <…>	
				<…> hasta <…>	
				Más de <…>	
8	Repositorio de paquetes de software			1 hasta <…>	
				<…> hasta <…>	
				<…> hasta <…>	
				<…> hasta <…>	
				Más de <…>	
9	Servicio de construcción e integración continua con Sistema operativo Linux.			1 hasta <…>	
				<…> hasta <…>	
				<…> hasta <…>	
				<…> hasta <…>	
				Más de <…>	
10	Recurso de cómputo con las siguientes características: 8 vCPU y 16 GB Memoria			1 hasta <…>	
				<…> hasta <…>	
				<…> hasta <…>	
				<…> hasta <…>	
				Más de <…>	
11	Registro de contenedores			1 hasta <…>	
				<…> hasta <…>	
				<…> hasta <…>	
				<…> hasta <…>	
				Más de <…>	
12	Servicio de autenticación Web/móvil			1 hasta <…>	
				<…> hasta <…>	
				<…> hasta <…>	
				<…> hasta <…>	
				Más de <…>	
13	Servicio de logs de la consola en nube			1 hasta <…>	
				<…> hasta <…>	
				<…> hasta <…>	
				<…> hasta <…>	
				Más de <…>	

Descripción del Servicio	Total (S/ Inc. IGV)
10.1. Servicios Compartidos	0.00
10.2. Ambiente de Producción	0.00
10.3. Ambiente de Certificación (QA)	0.00
10.4. Ambiente Desarrollo (DEV)	0.00
10.5. Componentes a Demanda	0.00
11.8. Especificaciones de Capacidades de los Servicios de Seguridad	0.00
Total General (S/ Inc. IGV)	0.00

10.1. Servicios Compartidos

Componentes del Servicio	Año 1 Costo (S/ Inc. IGV)	Año 2 Costo (S/ Inc. IGV)	Año 3 Costo (S/ Inc. IGV)	Total (S/ Inc. IGV)
Servicio de NAT Horas				
Conexión VPN Site to Site				
Conexión Cliente VPN				
Conector de redes en múltiples zonas				
Servicio de transferencia de datos				
Kit de desarrollo de software en la nube				
Servicio de entrega continua				
Repositorio de paquetes de software				
Servicio de construcción e integración continua con Sistema operativo Linux.				
Recurso de cómputo con las siguientes características: 8 vCPU y 16 GB Memoria				
Registro de contenedores				
Servicio de autenticación Web/móvil				
Servicio de logs de la consola en nube				
Total (S/ Inc. IGV)				0.00

10.2. Ambiente de Producción

Componentes del Servicio	Año 1 Costo (S/ Inc. IGV)	Año 2 Costo (S/ Inc. IGV)	Año 3 Costo (S/ Inc. IGV)	Total (S/ Inc. IGV)
Servicio de base de datos relacional compatible con PostgreSQL en alta disponibilidad (Primario/Respaldo) en multizona				
Cada característica puede consumirse de manera independiente				
Servicio de base de datos de documentos compatible con (mongoDB) Cada característica puede consumirse de manera independiente 2 Instancias, una por Zona de disponibilidad				
Servicio de administración y despliegue de APIs				
Balanceador de carga de red				
Servicio de contenedores basado en Kubernetes				
Servicio de máquinas virtuales de cómputo para kubernetes con Sistema operativo Linux				
Servicio de CDN				
Servicio de gestión de claves criptográficas				
Servicio de almacenamiento de secretos				

Servicio de almacenamiento de objetos				
Servicio de monitoreo y observabilidad				
SFTP				
Servicio de ejecución de Funciones sin servidor				
Total (S/ Inc. IGV)				**0.00**

10.3. Ambiente de Certificación (QA)

Componentes del Servicio	Año 1 Costo (S/ Inc. IGV)	Año 2 Costo (S/ Inc. IGV)	Año 3 Costo (S/ Inc. IGV)	Total (S/ Inc. IGV)
Servicio de base de datos relacional compatible con PostgreSQL en alta disponibilidad (Primario/Respaldo) en multizona				
Servicio de base de datos de documentos compatible con (mongoDB) Cada característica puede consumirse de manera independiente 2 Instancias, una por Zona de disponibilidad				
Servicio de administración y despliegue de APIs				
Balanceador de carga de de aplicación				
Servicio de contenedores basado en Kubernetes				
Servicio de máquinas virtuales de cómputo con Sistema operativo Linux				
Servicio de CDN				
Servicio de gestión de claves criptográficas				
Servicio de almacenamiento de secretos				
Servicio de almacenamiento de objetos				
Servicio de monitoreo y observabilidad				
SFTP				
Servicio de ejecución de Funciones sin servidor				
Total (S/ Inc. IGV)				**0.00**

10.4. Ambiente Desarrollo (DEV)

Componentes del Servicio	Año 1 Costo (S/ Inc. IGV)	Año 2 Costo (S/ Inc. IGV)	Año 3 Costo (S/ Inc. IGV)	Total (S/ Inc. IGV)
Servicio de base de datos relacional compatible con PostgreSQL				
Servicio de base de datos de documentos compatible con (mongoDB) Servicio de administración y despliegue de APIs				
Balanceador de carga de aplicación				
Servicio de contenedores basado en Kubernetes				
Servicio de máquinas virtuales de cómputo con Sistema operativo Linux				
Servicio de CDN				
Servicio de gestión de claves criptográficas				
Servicio de almacenamiento de secretos				

Servicio de almacenamiento de objetos				
Servicio de monitoreo y observabilidad				
SFTP				
Servicio de ejecución de Funciones sin servidor				
Total (S/ Inc. IGV)				**0.00**

10.5. Componentes a Demanda

Componentes del Servicio	Costo (S/ Inc. IGV)	Total (S/ Inc. IGV)
Servicio de base de datos relacional (HA)		
Servicio de base de datos de documentos		
Servicio de máquinas virtuales de cómputo para kubernetes con Sistema operativo Linux		
Direct Connet hosteado		
Total (S/ Inc. IGV)		**0.00**

11.8. Especificaciones de Capacidades de los Servicios de Seguridad

Componentes del Servicio	Año 1 Costo (S/ Inc. IGV)	Año 2 Costo (S/ Inc. IGV)	Año 3 Costo (S/ Inc. IGV)	Total (S/ Inc. IGV)
Consola SaaS de Seguridad para los servicios WAF, ataques volumétricos de denegación de servicio y servicio de seguridad de APIs.				
Plataforma de protección nativa de nube para aplicaciones (CNAPP)				
Servicio de Next Generation Firewall (NGFW)				
Total (S/ Inc. IGV)				**0.00**

ANEXO N° 4
Costo del Componente Opcional - Cuenta DNI
Implementación de la Nueva Plataforma Bancaria para los Canales Digitales Banca Móvil y Banca por Internet del Banco de la Nación

Ver Anexo N° 4 de los TDR del Requerimiento

Concepto	Escenarios Opcionales	Costo (S/ inc. IGV)*
Cuenta DNI	**Escenario 1:** El contratista deberá realizar el desarrollo correspondiente a fin de enlazar los servicios del APP con los recursos de nube donde se encuentra alojado Cuenta DNI. Se coordinará con el proveedor los accesos correspondientes y las pruebas necesarias.	0.00
	Escenario 2: La Cuenta DNI será considerada como una Cuenta BN y el Contratista deberá realizar el desarrollo a fin de dar el mismo tratamiento que a las demás cuentas que se encuentran registradas en el Core Bancario (Mainframe).	0.00

(*): El Contratista deberá considerar el monto máximo según escenario para la cotización consolidada

El precio de la oferta es en Soles (S/) incluye todos los tributos, los costos laborales conforme a la legislación vigente; así como, cualquier otro concepto que pueda tener incidencia sobre el costo del servicio a contratar.

[CONSIGNAR CIUDAD Y FECHA]

……..
Firma, Nombres y Apellidos del postor o
Representante legal o común, según corresponda

Importante

- ***El postor que goce de alguna exoneración legal, debe indicar que su oferta no incluye el tributo materia de la exoneración, debiendo incluir el siguiente texto:***

Mi oferta no incluye [CONSIGNAR EL TRIBUTO MATERIA DE LA EXONERACIÓN]".

Formato **Nº 7**

EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD

Señores
COMITÉ DEL CONCURSO DE MERITOS
Concurso de Méritos Nº 0004-2024-BN
Presente.-

Mediante el presente, el suscrito detalla la siguiente EXPERIENCIA EN LA ESPECIALIDAD*:*

Nº	CLIENTE	OBJETO DEL CONTRATO	N° CONTRATO / O/S / COMPROBANTE DE PAGO	FECHA DEL CONTRATO O CP [25]	FECHA DE LA CONFORMIDAD DE SER EL CASO	EXPERIENCIA PROVENIENTE[26] DE:	MONEDA	IMPORTE [27]	TIPO DE CAMBIO VENTA[28]	MONTO FACTURADO ACUMULADO[29]
1										
2										
3										
4										
5										
6										
	…									
TOTAL										

[CONSIGNAR CIUDAD Y FECHA]

……
Firma, Nombres y Apellidos del postor o
Representante legal o común, según corresponda

[25] Se refiere a la fecha de suscripción del contrato, de la emisión de la Orden de Servicios o de cancelación del comprobante de pago, según corresponda.

[26] Si el titular de la experiencia no es el postor, consignar si dicha experiencia corresponde a la matriz en caso que el postor sea sucursal, o fue transmitida por reorganización societaria, debiendo acompañar la documentación sustentatoria correspondiente, *"Considerando que la sociedad matriz y la sucursal constituyen la misma persona jurídica, la sucursal puede acreditar como suya la experiencia de su matriz"*. Del mismo modo, *"… en una operación de reorganización societaria que comprende tanto una fusión como una escisión, la sociedad resultante podrá acreditar como suya la experiencia de la sociedad incorporada o absorbida, que se extingue producto de la fusión; asimismo, si en virtud de la escisión se transfiere un bloque patrimonial consistente en una línea de negocio completa, la sociedad resultante podrá acreditar como suya la experiencia de la sociedad escindida, correspondiente a la línea de negocio transmitida. De esta manera, la sociedad resultante podrá emplear la experiencia transmitida, como consecuencia de la reorganización societaria antes descrita, en los futuros procesos de selección en los que participe"*.

[27] Se refiere al monto del contrato ejecutado incluido adicionales y reducciones, de ser el caso.

[28] El tipo de cambio venta debe corresponder al publicado por la SBS correspondiente a la fecha de suscripción del contrato, de la emisión de la Orden de Servicios o de cancelación del comprobante de pago, según corresponda.

[29] Consignar en la moneda establecida en las bases.

Formato **Nº 8**

DECLARACIÓN JURADA DE REORGANIZACION SOCIETARIA

Señores
COMITÉ DEL CONCURSO DE MERITOS
Concurso de Méritos Nº 0004-2024-BN
Presente.-

Mediante el presente el suscrito, Representante Legal de [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA], declaro que la experiencia que acredito de la empresa [CONSIGNAR LA DENOMINACIÓN DE LA PERSONA JURÍDICA] absorbida como consecuencia de una reorganización societaria, no se encuentra sancionada.

[CONSIGNAR CIUDAD Y FECHA]

.....
Firma, Nombres y Apellidos del postor o
Representante legal, según corresponda

Formato **Nº 9**

AUTORIZACIÓN DE NOTIFICACIONES DE LA ENTIDAD (BANCO DE LA NACION) DURANTE LA EJECUCION CONTRACTUAL MEDIANTE MEDIOS ELECTRÓNICOS DE COMUNICACIÓN

(DOCUMENTO A PRESENTAR EN EL PERFECCIONAMIENTO DEL CONTRATO)

Señores
BANCO DE LA NACION
Presente.-

El que se suscribe, [……..], Representante Legal de […….], identificado con [CONSIGNAR TIPO DE DOCUMENTO DE IDENTIDAD] N° [CONSIGNAR NÚMERO DE DOCUMENTO DE IDENTIDAD], autorizo al Banco de la Nación que se me notifique al correo electrónico [INDICAR EL CORREO ELECTRÓNICO], las notificaciones que se realicen durante la etapa de ejecución del contrato suscrito entre ambas partes.

[CONSIGNAR CIUDAD Y FECHA]

……
Firma, Nombres y Apellidos del postor o Representante legal, según corresponda

Formato Nº 10

(Si es Persona Jurídica)

DECLARACIÓN JURADA
RESOLUCIÓN SBS N° 2660-2015 - REGLAMENTO DE GESTIÓN DE RIESGOS DE LAVADO DE ACTIVOS Y DEL FINANCIAMIENTO DEL TERRORISMO

Señores
BANCO DE LA NACIÓN
CONCURSO DE MERITOS Nº 0004-2024-BN
Presente.-

[CONSIGNAR NOMBRE DE LA EMPRESA], con Registro Único de Contribuyentes Nº [CONSIGNAR], con domicilio legal en [CONSIGNAR], distrito de [CONSIGNAR], provincia y departamento de [CONSIGNAR], debidamente representada por su apoderado, el señor [CONSIGNAR], identificado con Documento de Identidad Nº [CONSIGNAR], cuyo poder obra inscrito en la Partida Electrónica Nº [CONSIGNAR], del Registro de Personas Jurídicas de [CONSIGNAR], declaro bajo juramento:

Conocer que EL BANCO DE LA NACIÓN es una Entidad Financiera sujeta al cumplimiento del Reglamento de Gestión de Riesgos de Lavado de Activos y del Financiamiento del Terrorismo, aprobado por Resolución SBS Nº 2660-2015, y que por tanto se obliga a proporcionar toda aquella información necesaria a fin de dar cumplimiento a lo dispuesto en los artículos 36º y 37º del referido Reglamento, así como a cualquier otra norma legal sobre la materia desde su entrada en vigencia, para lo cual se compromete a presentar con carácter obligatorio la siguiente documentación para la firma del contrato, la misma que se detalla:

SI ES PERSONA JURÍDICA:

Por el presente documento, declaro bajo juramento, lo siguiente:				
PERSONA JURÍDICA:				
1	Denominación o razón social:			
2	Número de RUC:		Número de Registro equivalente, para no domiciliados:	
3	Dirección de la oficina o local principal donde desarrolla las actividades propias del negocio (Indicar: Jr. - Av. - Calle - Pasaje / N° / Dpto-Int. N° /Urb. - Complejo - Zona – Sector /Distrito/Provincia/Departamento):			
4	Rubros en los que el proveedor brinda sus productos o servicios:			
5	Años de experiencia en el mercado:			
6	Se encuentra incluida en la lista emitida por la Oficina de Control de Activos Extranjeros del Departamento de Tesoro de los Estados Unidos de América (OFAC) SI ☐ - NO ☐			
7	**Representante legal:**			
	Nombres y Apellidos:			
	Tipo y número de documento de identidad **(marque con una "X" según corresponda).**			
	DNI ( )	Pasaporte ( )	Carné de Extranjería ( )	Otro (Indique):
	Domicilio (Indicar: Jr. - Av. - Calle - Pasaje / N° / Dpto-Int. N° /Urb - Complejo - Zona – Sector /Distrito/Provincia/Departamento):			
	Rubros en los que el proveedor brinda sus productos o servicios:			
	Años de experiencia en el mercado:			
	Contar con antecedentes penales ( ) No contar con antecedentes penales ( )			

	Se encuentra incluido en la lista emitida por la Oficina de Control de Activos Extranjeros del Departamento de Tesoro de los Estados Unidos de América (OFAC) SI ☐ - NO ☐			
8	**Identificación de los accionistas, socios o asociados, que tengan directa o indirectamente <u>más del 25%</u> del capital social, aporte o participación de la persona jurídica. <u>Respecto de cada uno de ellos</u>, se debe indicar:**			
	En caso el accionista, socio o asociado sea persona natural:			
	Nombres, Apellidos y porcentaje del capital social: 1. 2.			
	Tipo y número de documento de identidad (marque con una "X" según corresponda).			
	DNI ( ) 1. 2	Pasaporte ( ) 1. 2	Carné de Extranjería ( ) 1. 2	Otro (Indique): 1. 2
	Contar con antecedentes penales ( ) No contar con antecedentes penales ( ) De marcar SI, detallar Nombre y Apellidos de dicho (s) accionista (s), socio (s) o asociado (s), que cuenta con antecedentes penales:			
	Se encuentran incluidos en la lista emitida por la Oficina de Control de Activos Extranjeros del Departamento de Tesoro de los Estados Unidos de América (OFAC) SI ☐ NO ☐ De marcar SI, detallar Nombre y Apellidos de dicho (s) accionista (s), socio (s) o asociado (s), que se encuentra en la Lista OFAC:			
	En caso el accionista, socio o asociado sea persona jurídica:			
	Denominación o razón social:			
	Número de RUC:	Número de Registro equivalente, para no domiciliados:		
	Dirección de la oficina o local principal donde desarrolla las actividades propias del negocio (Indicar: Jr. - Av. - Calle - Pasaje / N° / Dpto-Int. N° /Urb. - Complejo - Zona – Sector /Distrito/Provincia/Departamento):			
	Años de experiencia en el mercado y rubros en los que el proveedor brinda sus productos o servicios:			
	Se encuentra incluido en la lista emitida por la Oficina de Control de Activos Extranjeros del Departamento de Tesoro de los Estados Unidos de América (OFAC) SI ☐ - NO ☐			
	N° Teléfono:			

Afirmo y ratifico todo lo manifestado en la presente declaración jurada y me comprometo a presentarla cada dos (02) años de ejecución contractual	**NOMBRE:**	
	FIRMA:	
	FECHA (día/mes/año):	/ /

*Importante:
- Cuando se trate de consorcios, la presente Declaración Jurada debe ser presentada por cada uno de los integrantes del consorcio.
- La información debe ser completada en su **totalidad**.

Formato **Nº 11**

FORMATO DE DECLARACIÓN JURADA DE NO ENCONTRARSE INSCRITO EN EL REGISTRO DE DEUDORES DE REPARACIONES CIVILES (REDERECI)

Señores
BANCO DE LA NACIÓN
Presente.–

Yo [CONSIGNAR NOMBRES Y APELLIDOS COMPLETOS] identificado con documento de identidad N° [CONSIGNAR NÚMERO DE DNI O DOCUMENTO DE IDENTIDAD ANÁLOGO], domiciliado en [CONSIGNAR EL DOMICILIO LEGAL], representante legal del postor [CONSIGNAR EL NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL POSTOR], declaro no encontrarme inscrito en el Registro de Deudores de Reparaciones Civiles (REDERECI) y, por lo tanto, de no contar con ninguno de los impedimentos establecidos en el artículo 5[30] de la Ley N° 303531 (Ley que crea el Registro de Deudores de Reparaciones Civiles - REDERECI) para acceder al ejercicio de la función pública y contratar con el Estado.

En caso de resultar falsa la información que proporciono, me sujeto a los alcances de lo establecido en el artículo 411 del Código Penal, concordante con el artículo 33 del Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General, aprobado por el Decreto Supremo N° 006-2017-JUS.

En mérito a lo expresado, firmo el presente documento.

[CONSIGNAR CIUDAD Y FECHA]

……..
Firma, Nombres y Apellidos del postor o
Representante legal o común, según corresponda

[30] **Artículo 5. Impedimento para acceder al ejercicio de la función pública y contratar con el Estado**

Las personas inscritas en el REDERECI están impedidas de ejercer función, cargo, empleo, contrato o comisión de cargo público, así como postular y acceder a cargos públicos que procedan de elección popular. Estos impedimentos subsisten hasta la cancelación íntegra de la reparación civil dispuesta.

Lo dispuesto en el párrafo anterior es inaplicable a las personas condenadas por delitos perseguibles mediante el ejercicio privado de la acción penal.

Formato **Nº 12**

DECLARACIÓN JURADA DE NO ESTAR INHABILITADO PARA CONTRATAR CON EL ESTADO

SEÑORES:
BANCO DE LA NACIÓN

De nuestra consideración:
Mediante el presente, el/la Sr./Sra. …….. identificado/a con DNI N° ……Representante Legal de la empresa …… con domicilio en **[CONSIGNAR INFORMACION DEL CONTRATISTA PERSONA JURIDICA O NATURAL]**……... con número telefónico ……. **[CONSIGNAR INFORMACION DEL CONTRATISTA PERSONA JURIDICA O NATURAL]** y RUC N°……**[CONSIGNAR INFORMACION DEL CONTRATISTA PERSONA JURIDICA O NATURAL]**
A nombre propio y de la empresa …… a la cual represento, **DECLARO BAJO JURAMENTO** lo siguiente:

1. No tener impedimento para ser postor y/o contratar con el Estado, conforme al artículo 11 de la Ley de Contrataciones del Estado.
2. Conocer, aceptar y someterme a los términos de referencia de la contratación.
3. Ser responsable de la veracidad de los documentos e información que presento a efectos del presente requerimiento.
4. Conocer las sanciones contenidas en la Ley de Contrataciones del Estado y su Reglamento, así como en la Ley Nº 27444, Ley del Procedimiento Administrativo General.

Ciudad, ……de …… del 20...

_____
Firma del Representante Legal

Importante
Aquellos socios, accionistas, participacionistas o titulares, de vuestra empresa que tengan participación individual o conjunta superior al 30% del capital o patrimonio social en otra empresa con el mismo objeto social, deberán suscribir de manera individual la presente declaración jurada, adjuntado la ficha RUC de la empresa que forman parte, siendo vuestra empresa responsable sobre la veracidad de dicha información. Tratándose de consorcio, la declaración jurada es presentada por cada persona natural y/o jurídica integrante del consorcio.